TECHNOLOGY,

THE ACQUISITIONS LOOP,

AND STRATEGIC PARALYSIS

BY

LT COL CHRIS KEITHLEY

A THESIS PROVIDED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2015

APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

____

M.V. Smith, Colonel, USAF (PhD) 1 May 2015

____

Richard Bailey, Colonel, USAF (PhD) 1 May 2015

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the United States Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Lt Col Chris Keithley was a 2000 graduate of the United States Air Force Academy where he majored in aeronautical engineering. Since commissioning, he has been assigned in operational, training, and experimental flight test squadrons. He is a graduate of the National Intelligence University for intermediate developmental education where he studied strategic intelligence. Most recently he mastered strategic studies at the School of Advanced Air and Space Studies.

ACKNOWLEDGMENTS

I would like to thank my thesis advisor Colonel M.V. “Coyote” Smith for his candor, support, and enthusiasm. I also wish to thank my parents for encouraging me to be curious about the world around me. Finally, this thesis would not have been possible without the unwavering encouragement of my fiancée, who has supported me from afar the last two years.

ABSTRACT

This thesis explores the relationship between military technology and strategic risk. As weapons become more dependent upon technology, they generally become more capable but at the same time introduce a new set of vulnerabilities. These vulnerabilities invite an adversary to conduct an attack that prevents the weapon from functioning properly. Because of the highly complex and integrated nature of America's military arsenal, such an attack could be particularly problematic and result in strategic paralysis. When such an attack occurs, the acquisitions process will be a determining factor in restoring full capability to the weapon system.

This study examines measures the United States can take to minimize the effects of such an attack. Specifically, recommendations regarding weapon system architecture and acquisition processes are considered.

CONTENTS

FIGURES

Chapter 1

Introduction

In the year 2054, the entire defense budget will purchase just one aircraft. This aircraft will have to be shared by the Air Force and Navy 3½ days each per week except for leap year, when it will be made available to the Marines for the extra day.
Norm Augustine, former Lockheed Martin CEO

The objective of this work is to explore the relationship between military technology and strategic risk. As weapons become more dependent upon technology, they generally become more capable while but at the same time introduce a new set of vulnerabilities. In the event an adversary attacks one of these vulnerabilities, the United States is compelled to respond in order to maintain the utility of the weapon system. Often, this response relies on the speed and agility of the acquisitions process. A slow response can dramatically enhance the effects of an otherwise small attack and lead to strategic paralysis. Therefore, this study poses the following question: Does the military's growing reliance on technology translate into a strategic liability?

Former British Army Captain Basil Liddell Hart argued that the aim of a strategist is not so much to seek battle as to seek an advantageous strategic situation.[1] Such a favorable scenario will not be realized by directly confronting an opponent, because doing so "consolidates his balance, physical and psychological, and by consolidating it increases his resisting power."[2] Instead, Liddell Hart recommends taking an indirect approach along the line of least

[1] B. H. Liddell Hart, *Strategy*, 2nd Rev. ed. 1967 (Reprint, New York: Penguin, 1991), 325.
[2] Hart, *Strategy*, 327.

resistance.[3] Regardless of the course a strategist chooses, the chosen plan should always account for the enemy's ability to frustrate it.[4]

Liddell Hart's conception of the indirect approach is increasingly relevant for the United States because of how its military relies upon technology. Today's weapon systems are highly reliant on computers and the code that runs them. These systems are also highly integrated both individually and collectively. By nature of their complex design, these systems afford potential adversaries more access points for hostile intrusion. Unfortunately, many of these access points may be unknown to the owner and are consequently undefended. In the parlance of cyber warfare, an unknown and undefended vulnerability is referred to as a "zero day exploit."[5]

Most importantly, some of these access points can provide an adversary the ability to cripple a particular weapon system, degrade its usefulness in combat, or make it more vulnerable to attack. Indeed, the counter to an attack of this nature can be a simple modification of tactics. In a worst-case scenario however, the workaround is much more involved, requiring modification to software and potentially even hardware. For the United States, this situation has particularly significant implications involving time, money, and combat effectiveness.

Furthermore, while such an upgrade or modification is in progress, combatant commanders will be denied the capabilities ordinarily offered by the sidelined platforms. Air Force doctrine is crafted carefully to provide airpower's unique benefits with flexibility and versatility, as outlined by the tenets of airpower in Air Force Doctrine Document-1

---

[3] Hart, *Strategy*, 327.
[4] Hart, *Strategy*, 330.
[5] P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York, NY: Oxford University Press, 2014), 115.

(AFDD-1).[6] With one or more platforms out of the fight, America would be operating at a doctrinal disadvantage.

The American military is presently the most technologically advanced in the world and continues to grow even more reliant on advanced weaponry.[7] However, as suggested by Norm Augustine, former chief executive of defense contractor Lockheed-Martin, the cost to develop and build the advanced weapon systems for the American military is growing at a rate faster than that of the defense budget.[8] Partially, as a result of this cost growth, the gap between what the military initially plans to procure, and what it actually acquires, is increasing.[9] Despite these smaller numbers, the military's reliance on technology continues to grow.

For strategists, the above implications matter enormously. In the extreme, the crippling of a low density, high demand platform could result in strategic paralysis. The likelihood of this is affected by decisions made in the platform's design as well as by the process used to upgrade or modify the system. For this reason, what follows explores the strategic relationship of technology to risk, surprise, and flexible response.

Definitions

[6] United States Air Force, "Air Force Basic Doctrine, Organization, and Command," October 14, 2011, 37, http://www.au.af.mil/au/cadre/aspc/l002/pubs/afdd1.pdf. The seven tenets of airpower are (1) Centralized control and decentralized execution, (2) Flexibility and versatility, (3) Synergistic effects, (4) Persistence, (5) Concentration, (6) Priority, and (7) Balance.

[7] Keith L. Shimko, *The Iraq Wars and America's Military Revolution* (New York, NY: Cambridge University Press, 2010), 218–220.

[8] Norman R. Augustine, *Augustine's Laws*, 6th ed (Reston, VA: American Institute of Aeronautics and Astronautics, 1997), 107.

[9] According to a 2010 RAND Corporation report titled *Ending F-22A Production: Costs and Industrial Base Implications of Alternative Options*, the United States Air Force initially sought to purchase 750 F-22 aircraft. Only 195 were built, 187 of which were fielded. Similarly, 21 B-2 bombers were built despite an expressed need for 132 according to a 1991 RAND report titled *Analysis of Air Force Aircraft Multiyear Procurements with Implications for the B-2*.

As with any academic study, defining the terms used aids in scoping the discussion as well as qualifying the applicability of the conclusions and recommendations. An understanding of the following terms is necessary to appreciate fully the arguments presented in this particular analysis.

Technology

This term can mean a number of different things based on the context in which it is used. Merriam-Webster's Collegiate dictionary defines technology as "a capability given by the practical application of knowledge."[10] In the context of weapon systems, both the stirrup and a GPS satellite satisfy that definition of technology.[11] For the purposes of this thesis however, the Merriam-Webster's definition is used as a foundation with the scope further restricted to include only those capabilities that require the proper functioning of modern computing hardware for successful employment.[12] For example, a carburetor-equipped World War II era Jeep would be excluded from this discussion whereas a modern vehicle with a computer-controlled fuel injection system would be included.

Vulnerability

The Department of Defense (DoD) Dictionary of Military and Associated Terms (Joint Publication (JP) 1-02) defines vulnerability at three levels. The first applies to a policy maker or combatant commander in that it defines the macro-effect of losing war-making capability: "the susceptibility of a nation or military force to any action by any means

---

[10] Merriam-Webster, Inc, *Merriam-Webster's Collegiate Dictionary*, 11th ed (Springfield, Mass: Merriam-Webster, Inc, 2003), 1283.
[11] Patrice. Flichy, *Understanding Technological Innovation: A Socio-Technical Approach* (Cheltenham, UK; Northampton, MA: Edward Elgar, 2007), 23.
[12] An implied assumption is that properly functioning modern computing hardware requires supporting software whose purpose is to control the processes executed by the hardware.

through which its war potential or combat effectiveness may be reduced or its will to fight diminished."[13] The second definition describes the system-level attributes and the meso-effects of an attack: "the characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (man-made) hostile environment."[14] The third definition presented in JP 1-02 highlights attributes inherent to a particular system or operational characteristics that are the access points for an adversary: "in information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system."[15] This can be considered the effects of vulnerability at the micro-level.

For the purposes of this analysis, an adversary's attack can only have strategic effect if it satisfies each of the three definitions in reverse order. If a system has no inherent weaknesses, there cannot be any attack degrading the system's functionality. Therefore, there will not be any associated decrease in combat effectiveness. The World War II era Jeep above is an example of a system that has no access points for a technological attack. Conversely, the Stuxnet computer virus attacked access points of Iranian nuclear enrichment centrifuge systems and realized effects at all three levels.[16]

A vulnerability whose effects are realized at all three levels is considered a critical vulnerability. This is consistent with the definition of critical vulnerability provided by both John Gentry and the DoD

---

[13] "Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms," November 14, 2014, 266, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
[14] "JP 1-02," 266.
[15] "JP 1-02," 266.
[16] Singer and Friedman, *Cybersecurity and Cyberwar*, 114–120; Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Do About It*, 1st Ecco pbk. ed (New York: Ecco, 2012), 291–296.

Dictionary of Military and Associated Terms. According to Gentry, an exploited critical vulnerability will "significantly alter strategic outcomes."[17] The definition in JP 1-02 is similar: an attribute "which is deficient or vulnerable to direct or indirect attack that will create decisive or significant effects."[18] This study will consider critical vulnerabilities using the JP 1-02 definition because of its broader applicability.

Risk

Accepted as defined by JP 1-02, risk is the "probability and severity of loss linked to hazards."[19] Risk management is defined as the "process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits."[20]

For a technologically advanced weapon system, risk management largely occurs during two critical timeframes. The first is throughout the acquisition process. During this period, risk changes result from the establishment of design specifications as well as when trades are made to satisfy cost, schedule, or performance requirements. Risk management is also an essential aspect of the operational planning process. There, a weapon system's exposure to risk changes as strategists determine what weapon systems to use and how to use them in a particular operation or campaign. Underlying the risk during the operational process is the speed at which the system can be upgraded or modified. A system that can be upgraded or modified quickly may be able to accept more short term risk than weapon systems that cannot.

---

[17] John A. Gentry, *How Wars Are Won and Lost: Vulnerability and Military Power* (Santa Barbara, CA: Praeger Security International, 2012), 3.
[18] "JP 1-02," 58.
[19] "JP 1-02," 217.
[20] "JP 1-02," 217.

Surprise

The incoming United States Air Force Academy class of 2000 learned in their student handbook, *Contrails,* that in order to surprise an adversary, one should "strike the enemy at a time or place or in a manner for which he is unprepared."[21] An attack on an unknown critical vulnerability of a weapon system is sure to be surprising for the strategist. Related to the doctrinal conception of surprise is the concept of strategic paralysis.

Modern day airpower theorists Col John Boyd and Col John Warden both appreciated the utility of strategic paralysis, which seeks to disable the enemy through the minimum effort or cost in lieu of physically destroying the enemy.[22] Technologically advanced weapon systems are vulnerable to adversaries equipped with extraordinarily inexpensive means, provided the adversary has sufficient access to conduct an attack. Because of this, the threat of strategic paralysis naturally grows the more advanced weapon systems become.

Flexible Response

Modern Airmen have embraced the concept that "flexibility is the key to airpower." The United States Air Force (USAF) also appreciates the value of flexibility and seeks to maintain the ability to respond to a wide range of contingencies.[23] This idea most closely resembles the DoD Dictionary definition of flexible response: "the capability of military forces for effective reaction to any enemy threat with actions appropriate and

---

[21] United States Air Force Academy, *Contrails*, vol. 1996–1997 (USAFA, CO, 1996), 45. This definition is consistent with that provided by Air Force Basic Doctrine, Organization, and Command.
[22] David S. Fadok, "John Boyd and John Warden: Air Power's Quest for Strategic Paralysis" (School of Advanced Airpower Studies, 1995), 10.
[23] Dag Henriksen, *NATO's Gamble: Combining Diplomacy and Airpower in the Kosovo Crisis, 1998-1999* (Annapolis, MD: Naval Institute Press, 2007), 31.

adaptable to the circumstances existing."[24] If an adversary attacks a critical vulnerability of a technologically advanced weapon system, the target's ability to respond flexibly will be severely degraded. In such a scenario, the strategist will be denied what the modern Airman maintains is the cornerstone of airpower.

Integration

This term can carry many contextually specific meanings. For the discussion that follows, the term's use will be constrained to the definition of how a system is designed and/or incorporated with other systems. To illustrate what integration is, it is helpful to first consider the concept of federation in the context of an aircraft cockpit.

Compare the images of the two cockpits below. The first image is from a small private airplane, a Cessna 172, from decades past and provides an example of a federated system. Each of the instruments is connected to a dedicated sensor and displays a single discrete piece of information to the pilot.

Figure 1: Cessna 172R Cockpit Poster

Source: Sporty's Pilot Shop

[24] "JP 1-02," 93.

Two major drawbacks to the federated approach led to its demise. First, the tasks of receiving and prioritizing incoming data and reconciling data conflicts were left to the pilot. As the volume of data flowing to the pilot increased, this became overwhelming in many cases. Second, as new sensors were added to aircraft, each would require a dedicated display.[25] Again, as the number of sensors increased, this became an increasingly intractable problem.

Figure 2 below depicts an F-22 cockpit, and is an example of an integrated cockpit. In this approach, the task of receiving and prioritizing the incoming information is accomplished by the computer code interpreting the sensor outputs. Additionally, the displays are generic and provide information from many sensors, some of which have themselves been combined to save weight and/or space. While integrating an aircraft cockpit transformed the way information is presented to the pilot, the computational framework required to do so created access points through which an adversary might attack the platform.

---

[25] David C. Aronstein, Michael J. Hirschberg, and Albert C. Piccirillo, *Advanced Tactical Fighter to F-22 Raptor Origins of The 21st Century Air Dominance Fighter* (Reston, Va.: American Institute of Aeronautics and Astronautics, 1998), 171–172.

Figure 2: F-22 Cockpit Layout
Source: F-22 Capabilities Briefing, 422 Test and Evaluation

Integrating many different platforms together to share battlespace information has similar benefits and has been an ongoing DoD effort for several decades. First introduced by Vice Admiral Arthur Cebrowski and John Garstka in 1998, the concept of Network-Centric Warfare (NCW) is defined as “an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace."[26]

The GPS constellation is an example of a platform that the NCW concept highly relies on. The military's dependence on GPS manifests itself at each of vulnerability's three levels discussed earlier. Not only do many of today's weapons rely on GPS to achieve their desired effects, but the system's capabilities also affect what weapons we procure and in what quantities we procure them. If information from a ubiquitous platform such as the GPS constellation is denied or adversely affected, strategic paralysis could indeed be the consequence.

Limitations of the Evidentiary Base

Unfortunately, this study lacks the ability to point to a particular event where a nation was strategically paralyzed by an asymmetric threat as a result of an attack on technologically advanced weapon systems. Therefore, the evidence chosen to support the hypothesis must have sufficient applicability to enough weapon systems to be generalizable. This guarantees that the evidence chosen does not represent an outlier, and will also ensure the subsequent recommendations are relevant to a diverse range of weapon systems. The characteristics of the systems used in the case studies are representative of overall trends in weapon systems to meet these evidentiary criteria.

Similarly, the study lacks the ability to identify particular vulnerabilities or zero-day exploits on the platforms discussed that have not been attacked. Instead, the study assumes that these vulnerabilities exist. While it is entirely possible that some of the vulnerabilities are

---

[26] Thomas X. Hammes, *The Sling and The Stone: On War in The 21st Century* (Minneapolis, MN: Zenith, 2006), 7; Arthur K. Cebrowski and John H. Garstka, "Network-Centric Warfare - Its Origin and Future," *Proceedings Magazine*, January 1998, http://www.usni.org/magazines/proceedings/1998-01/network-centric-warfare-its-origin-and-future.

known and protected, it is highly unlikely that all are known and protected.[27]

One would expect data describing current system vulnerabilities to be classified. For this reason, this analysis relies on available historical data to illustrate the argument. Implicitly, it also assumes that future upgrades or modifications to a technologically advanced weapon system after a wartime attack would have a similar time and cost requirement as the peacetime equivalents presented in the case studies.

Recent years have seen prognostications of an impending "cyber Pearl Harbor" or "cyber 9/11."[28] Fortunately, such a cataclysmic event has not occurred but neither has sufficient effort been invested in defending against such an attack. The American public, policymakers, and military are beginning to more fully appreciate the extent to which their nation relies on vulnerable technology.[29] In that spirit, this study seeks to explore how a more responsive and faster running acquisitions process can mitigate some of the risks associated with these vulnerabilities.

Methodology

This study begins with a literature review of the relevant theoretical base. Its conclusions and recommendations rely heavily on that review as well as multiple interviews with professionals in the Air Force's test and evaluation discipline. Their perspective was especially useful because it provided real-world examples of the phenomenon being investigated.

The theory presented in Chapter 3 leverages John Boyd's observe, orient, decide, act model, commonly referred to as the OODA loop.

---

[27] Admittedly, this assertion is made without any data that identifies specific vulnerabilities. Nonetheless, the assertion is reasonable in light of the overwhelming number of systems that share similar computing architecture (hardware and software) that do have vulnerabilities of this nature.
[28] Singer and Friedman, *Cybersecurity and Cyberwar*, 37.
[29] Singer and Friedman, *Cybersecurity and Cyberwar*, 151.

Technology's relationship to the OODA loop is increasingly relevant, as this study demonstrates. Case studies will be conducted using both the F-22 and the Global Positioning System. These particular systems were chosen because of how their vulnerabilities affect overall risk.

Overview

Chapter 2 will more thoroughly explore the problem and its setting, beginning with a discussion of how the proliferation of advanced weapon systems satisfied social pressures to minimize the expense of war. Four important implications of the move towards technology are presented. Building upon each other, they culminate in highlighting how the speed at which American weapon systems can be upgraded or modified is a critical vulnerability. Chapter 3 begins by establishing the theoretical relevance of the situation. It then explores recommendations made by two Defense Science Board studies and offers three additional recommendations, all of which seek to accelerate the speed of the acquisitions loop. The first case study appears in Chapter 4. Using data provided by the F-22 program, it explores the demands required to modify a highly integrated modern weapon system. There we will see that the challenges associated with modifying a single platform are daunting and worthy of the strategist's attention. These challenges are further amplified for a platform that interacts with many other platforms. To illustrate this particular point, the next case study in Chapter 5 examines GPS, highlighting how a single platform's vulnerabilities create risk across multiple other platforms and in all services and domains. Solutions proposed in Chapter 3 are tested against each case study to evaluate how the proposals affect each system's vulnerabilities. Finally, Chapter 6 summarizes this investigation's main concepts.

Chapter 2

Technology, Vulnerability, and Strategic Paralysis

Go into emptiness, strike voids, bypass what he defends, hit him where he does not expect you.
Sun Tzu

Regarding the conventional military power of the United States relative to the rest of the world, historian Paul Kennedy wrote that "nothing has ever existed like this disparity of power; nothing."[1] In his estimation, only a madman would attack a country with as much clout as America's.[2] Paradoxically though, recent decades have seen the United States in conflict with comparatively weak nation states as well as even weaker non-state actors. Though America's overwhelming military might has continued to grow, it has failed to deter some of its potential adversaries. Furthermore, when it has engaged these less capable foes, it routinely has failed in attaining swift and decisive victories. Technology's prevalence in the United States military may actually exacerbate instead of reverse this alarming trend.

What follows describes how America's military might became inextricably linked to technology as well as the implications of the phenomenon. Ultimately, the military's dependence upon technology results in growing vulnerabilities to the force and assumes increased risk in many areas. Understanding this dependence is crucial to understanding the relevance of the speed of the acquisitions loop.

[1] Paul Kennedy, "The Greatest Superpower Ever," *New Perspectives Quarterly* 19, no. 2 (Spring 2002): 5, http://www.digitalnpq.org/archive/2002_spring/kennedy.html.
[2] Paul Kennedy, "The Greatest Superpower Ever," 2.

How Did We Get Here?

The incredible military capability possessed by the United States is the confluence of two trends. The first is sociological, and the other is technical. Each is explored in turn.

Something for Nothing

War is expensive. It consumes the resources of a nation, draining it economically and socially. A leader whose nation does not have sufficient resources to wage war is less apt to seek it. For those leaders who do, they naturally seek to limit the scale, scope, or duration of conflict while still being able to achieve the desired political objectives. These limitations may serve economic interests as well as moral.

How a nation conducts itself in war is just as crucial as the decision to engage in conflict or not. For this reason, normative concepts developed over time that created boundaries for acceptable conduct in warfare. The just war theory is one such norm that incorporates many ideas including utility, proportionality, noncombatant immunity, military necessity, and neutrality.[3] Broadly understood, these normative structures are objective standards of conduct for and within conflict.

Globalization and the democratization of information have made it more difficult for nations to ignore these norms, effectively amplifying the importance of minimizing casualties and collateral damage in warfare. The worldwide expansion of electronic connectivity enables people and nations to witness the horrors of war much more easily than before.[4] Furthermore, the popular reaction to conflict matters, especially when a much larger audience witnesses conduct exceeding the bounds of

[3] Michael Walzer, *Just And Unjust Wars: A Moral Argument With Historical Illustrations*, 4th ed. (New York: Basic Books, 2006), vi.
[4] David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla*, 1 edition (Oxford ; New York, NY: Oxford University Press, 2013), 170; Emile Simpson, *War From the Ground Up: Twenty-First Century Combat as Politics* (Oxford ; New York, NY: Oxford University Press, 2012), 67–90.

established norms. This tendency is especially pronounced in democracies where public support for conflict tends to be inversely proportional to the number of casualties suffered.[5] As a result of these ramifications, modern leaders are more incentivized than their predecessors to end conflicts quickly and with minimal loss of life. Enabled by precision and lethality afforded by modern technology, they will pursue courses of action they believe will minimize the overall cost of a war while still attaining the desired objective.[6]

Technology Saves the Day

The second trend contributing to the overwhelming strength of the United States military, and the Air Force in particular, is technical. The same technological revolution that expanded electronic connectivity to the masses also fueled an explosion of advancement in weaponry. Developments in aviation illustrate how pervasive technology has become in modern weapon systems.

When Orville and Wilbur Wright left the beaches of Kitty Hawk, North Carolina on December 14, 1903, what they had accomplished was momentous. Mankind had finally achieved the centuries-long dream of powered flight.[7] "The technology that permits heavier-than-air manned flight is still with us, even if in all but technically unrecognizable detail from its fragile beginnings a century ago."[8]

During World War I (WWI), combat aircraft had wooden frames, fabric covered wings, and carbureted internal combustion engines. The pilots controlled the aircraft from an open cockpit via direct mechanical linkage to the flight controls. They dropped unguided gravity bombs

---

[5] Keith L. Shimko, *The Iraq Wars and America's Military Revolution* (New York, NY: Cambridge University Press, 2010), 32.
[6] Colin S. Gray, *Perspectives on Strategy*, 1st ed (Oxford, U.K: Oxford University Press, 2013), 180.
[7] Michael S Sherry, *The Rise of American Air Power: The Creation of Armageddon* (New Haven: Yale University Press, 1987), 1.
[8] Gray, *Perspectives on Strategy*, 183.

using their best judgment for sighting. Despite the comparative lack of sophistication, the aircraft of the day enabled Airmen to threaten targets behind the enemy's front lines for the first time in history. The new technology fostered a culture of optimism because it offered a solution to the seemingly intractable stalemates of trench warfare. "Over, not through" became the Airmen's motto.[9]

The descendants of these machines barely resemble their ancestors. Featuring advanced composite materials, modern aircraft are built using computer aided manufacturing techniques to exacting tolerances. They are propelled with jet engines whose computer controls extract the maximum amount of chemical energy out of the burned fuel. If the aircraft is manned, its pilot is situated in an enclosed, climate-controlled cockpit monitoring the output of sensor suites on digital avionics displays and communicating simultaneously with assets on the ground, in the air, or even in space. The pilot controls the aircraft via digital flight control systems. These "fly-by-wire" systems combine the pilot's commands with a number of other automated inputs into a computer-controlled output to the flight control surfaces. In effect, the pilot has been reduced to a voting member on the control of the aircraft, ceding the final decision to the computer software and hardware. Finally, the aircraft are equipped with a dizzying array of weapons including guided bombs and missiles, whose precision allows the pilot to discretely and reliably engage different targets separated by only inches. Each of these weapons is also outfitted with computer-controlled guidance systems, receiving target cueing from onboard aircraft computers.

Undoubtedly, technology is profoundly important to modern weapon systems. Many of the technologies incorporated onto them seek to increase the likelihood that the intended target is actually struck by

[9] Paula G. Thornhill, *Over Not Through: The Search for a Strong, Unified Culture for America's Airmen*, RAND Corporation Occasional Paper Series OP-386-AF (Santa Monica, CA: Rand, 2012), 3.

the weapon. Comparing the bombing performance during World War II (WWII) to today illustrates how computers have changed many of the fundamentals of how nations prepare for and approach armed conflict.

Before and during WWII, a number of technological advancements were made to improve navigation and targeting. Two of these developments included the Gee radar and the Norden bombsight.[10] Despite these and other improvements, precision bombing was anything but. In fact, mission planners incorporated performance metrics that are unthinkable today. Multiple bomber sorties with loaded bomb racks were sent to engage a single target, and often returned with their bombs expended but having failed to destroy the intended target. Moreover, some of those aircraft would be expected to be lost in the operation.[11]

Today, weapons have achieved "near surgical precision," according to Stephen Wrage.[12] The accuracy of modern navigation and targeting systems allows planners to think very differently than their WWII counterparts. "With guided munitions dramatically increasing the likelihood of a single sortie's success, it becomes possible to plan in terms of the number of targets per sortie, thus reversing the historical equation and making possible an economy of force never before seen in air war."[13]

Economy of force was not the only principle of war affected by precision weaponry. In addition to affecting how planners and practitioners alike thought about economy of force, the ability to precisely engage a target also had implications for how to think about

---

[10] Randall T. Wakelam, *The Science of Bombing: Operational Research in RAF Bomber Command* (Toronto ; Buffalo: University of Toronto Press, 2009), 59–61; Tami Davis Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas About Strategic Bombing, 1914-1945* (Princeton, N.J.: Princeton University Press, 2002), 161.
[11] Wakelam, *The Science of Bombing*, 226.
[12] Stephen Wrage, "Prospects for Precision Air Power," *Defense and Security Analysis* 19, no. 2 (2003): 102.
[13] Shimko, *The Iraq Wars and America's Military Revolution*, 81; George Friedman and Meredith Friedman, *The Future of War: Power, Technology and American World Dominance in the 21st Century* (New York: St. Martin's Griffin, 1998), 278.

achieving the effects of mass. What had historically required massing physical forces to reach the necessary concentration of combat power at the decisive place and time now required comparatively few.[14]

Significantly, the intent of these development efforts allowed precision engagement of targets while simultaneously satisfying the increasingly stringent requirements of prevailing moral and ethical strictures.[15] The social trend discussed at the opening of this chapter considered how norms developed intending to limit war's social effects. Extending this trend to the extreme would eliminate the need for a costly ground campaign where much of war's costs are incurred. The precision targeting capabilities provided by technological advancements suggest an expensive ground campaign may be unnecessary and that the dream of victory from the air is actually possible.[16]

The above describes how technology affected aviation, and bombing missions specifically, from WWII to today. Not surprisingly, technology's effects are not confined to that particular mission set. Instead, these changes are emblematic of overall advancements in weaponry and military systems across all domains during that same timeframe. From aircraft carriers to infantry platoons, mission sets in all of America's services rely on modern technology and have benefitted in similar ways as bombers. In many ways, the increased precision afforded by modern weapons satisfies the social mandate to minimize the effects of warfare.

Social conditions established a need for precision that technology was able to satisfy. Unfortunately, the significant benefits afforded by

---

[14] Frans P. B. Osinga, *Science, Strategy and War the Strategic Theory of John Boyd* (London; New York: Routledge, 2007), 249; John M. Shalikashvili, *Joint Vision 2010* (Washington, D.C: Chairman of the Joint Chiefs of Staff, July 1996), 17.
[15] Biddle, *Rhetoric and Reality in Air Warfare*, 161.
[16] Shimko, *The Iraq Wars and America's Military Revolution*, 57; Michael Kelly, "The American Way of War," *The Atlantic*, June 2002, http://www.theatlantic.com/magazine/archive/2002/06/the-american-way-of-war/302513/.

technology is not without cost. Modern technologically advanced weaponry now used by all of the services in their respective mission sets actually introduces vulnerabilities and increased risk.

Why Does It Matter?

The United States military relies on weapons that are increasingly technology-intensive. Four implications of this trend introduce vulnerabilities or amplify risk. Each implication is noteworthy individually. However, it is important to highlight that they have a cumulative effect and together are a veritable house of cards with a fragile foundation.

The first implication is that the systems have inherent vulnerabilities resulting from overly optimistic assumptions made in the design process. Some of these assumptions include the notion that generic computing hardware and millions of lines of code are impervious to adversary actions. Second, as the conventional American military grows increasingly stronger with technologically advanced weapon systems, the capability of the threat necessary to counter it does not grow at the same rate. Therefore, the asymmetry between the United States' capability and those of its potential adversaries actually grows. Third, advanced weaponry has changed how nations achieve principles such as mass and economy of force. Naturally, this phenomenon has affected force development and today determines what weapons are bought and in what quantities. Finally, when an adversary deploys a countermeasure affecting a weapon system capability, often times a modification is required to the system's hardware, software, or both. Such modifications rely on the speed of the acquisition loop, which will be shown to be of the utmost importance.

Each of these implications is explored in turn. The final implication is the only one that can easily be affected and will be what the recommendations offered in Chapter 3 seek to improve. Furthermore, the speed of the acquisitions loop will be the unit of measure for the case studies in Chapters 4 and 5. The speed of the acquisitions loop directly contributes to determining the severity of an adversary's attack.

Implication 1: The Open Door

In 2007, the Israeli Air Force conducted a successful airstrike on a Syrian nuclear reactor under construction. According to US intelligence analysts, radars protecting Syrian airspace went off the air while the raid was underway negating their ability to defend against the Israeli attack.[17] Though the details are not known, the available evidence points to the Israelis conducting a coordinated effort that included an attack on either the computing hardware or software of the Syrian air defenses.[18]

Earlier, technology was defined as a capability requiring the proper functioning of modern computing hardware. An assumption of that definition was that the hardware required supporting software to control the processes executed by the hardware. To impair or preclude the proper functioning of modern computing hardware, an adversary can attack the hardware, the software, or both. Unfortunately, vulnerabilities exist in both the hardware and software, offering a potential adversary several avenues of attack.

Many of the hardware vulnerabilities exist as a result of overall market trends. The market for military computing equipment is a small fraction of the total integrated circuit (IC) market.[19] Therefore, "nearly every military system today contains some commercial hardware," most of which is produced overseas.[20] Additionally, the hardware was not purpose-built for its particular application and often has many more

---

[17] David A. Fulghum, Robert Wall, and Amy Butler, "Cyber-Combat's First Shot," *Aviation Week & Space Technology* 167, no. 21 (November 26, 2007): 28–31.
[18] Fulghum, Wall, and Butler, "Cyber-Combat's First Shot."
[19] S. Adee, "The Hunt For The Kill Switch," *Spectrum, IEEE* 45, no. 5 (2008): 2, doi:10.1109/MSPEC.2008.4505310.
[20] Adee, "The Hunt For The Kill Switch," 1-2.

capabilities than is required by a particular system.[21] Due to time and resource constraints, it is impossible to test every single chip used by a particular weapon system.[22]

The combination of foreign-sourced generic computing hardware and an inability to detect sabotaged equipment caught the attention of the Defense Science Board that concluded in 2005 these otherwise sound industry changes presented long-term national security challenges.[23] The board was especially concerned that no mechanism was available to detect chips that had been compromised.[24] Ultimately, the board's concerns spawned a Defense Advanced Research Projects Agency program named "Trust in IC" to address the issue.[25]

Vulnerabilities arguably exist in software to an even greater extent than they do in hardware. Software is written to control the processes executed by computing hardware. Therefore, an adversary could alter the code itself or the inputs to the code in order to generate a desired outcome. For instance, the Stuxnet virus was malicious software written to target Iranian nuclear centrifuge controllers specifically. The altered code modified the inputs in addition to the operation of the centrifuges themselves, ultimately causing them to self-destruct.[26]

The ubiquity of technology in American weaponry is not lost on America's potential adversaries. Two officers in China's People's Liberation Army underscore the idea that an overreliance on technology can turn technical advantage into a liability: "Who now dares state with certainty that in future wars this heavy spending will not result in an

---

[21] Adee, "The Hunt For The Kill Switch," 5.
[22] Adee, "The Hunt For The Kill Switch," 2.
[23] Defense Science Board, *Defense Science Board Task Force On High Performance Microchip Supply*, February 2005, 3, http://www.acq.osd.mil/dsb/reports/ADA435563.pdf.
[24] Defense Science Board, *Defense Science Board Task Force On High Performance Microchip Supply*, 3.
[25] Adee, "The Hunt For The Kill Switch," 3.
[26] Singer and Friedman, *Cybersecurity and Cyberwar*, 114–120; Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Do About It*, 1st Ecco pbk. ed (New York: Ecco, 2012), 116–117.

electronic Maginot Line that is weak because of its excessive dependence on a single technology?"[27]

Implication 2: Strength Versus Vulnerability

As the United States' military capabilities continue to grow, they do so with an emphasis on technology. The reliance on technology is expensive, with the United States outspending the next nine countries on defense in 2014.[28] Some argue that America's reliance on technology constitutes a revolution in military affairs (RMA) that is as profound a change in warfare as the introduction of gunpowder.[29]

Andrew Krepenevich defines an RMA as "what occurs when the application of new technologies into a significant number of military systems combines with the innovative operational concepts and organizational adaptations in a way that fundamentally alters the character and conduct of conflict. It does so by producing a dramatic increase – often an order of magnitude or greater – in the combat potential and military effectiveness of armed forces."[30] The increase in combat potential and effectiveness understandably has implications for the adversary.

For many of America's potential adversaries, copying America's military is neither technologically feasible nor is it cost effective. Therefore, the preferred option is countering, which seeks to obviate American capabilities with asymmetric solutions that are relatively low

---

[27] Liang, Qiao and Xiangsui, Wang, *Unrestricted Warfare* (Beijing, China: PLA Literature and Arts Publishing House, February 1999), 87, http://www.terrorism.com/documents/unrestricted.pdf.
[28] Guy Eastman and Fenella McGerty, "US No Longer Spends More on Defense than Next 10 Biggest Countries Combined," *IHS Jane's 360*, June 25, 2014, http://www.janes.com/article/40083/analysis-us-no-longer-spends-more-on-defense-than-next-10-biggest-countries-combined.
[29] Shimko, *The Iraq Wars and America's Military Revolution*, 2.
[30] Andrew F. Krepinevich, Jr., "Cavalry to Computer: The Pattern of Military Revolutions," The National Interest, Fall 1994, p. 30.

cost without requiring advanced technologies.[31] The ability of a potential adversary to develop expertise in cyberspace appears to be a "considerable leveler of capabilities between otherwise grossly asymmetric security communities."[32]

This same cost-benefit calculation is illustrated by the Israeli attack on Syrian nuclear facilities. Israel went to the trouble of performing the cyber attack on the Syrian air defense system. At face value, this can be interpreted to mean that a properly operating air defense system may have otherwise deterred the attack. Other means to attack the system were beyond the reach of the Israelis. For instance, they lack the military-industrial capacity to produce stealth assets like the B-2 that are necessary to penetrate air defense systems.[33] Therefore, the Israelis were forced to attack the air defense system via other means that were within their capabilities.[34]

As illustrated by this example, the propensity of an overmatched adversary to seek countermeasures that are cheap and comparatively easy to develop amplifies the risk posed by vulnerabilities introduced by a reliance on technology. This risk is further exacerbated by trends in force development.

Implication 3: Quantity Has a Quality All Its Own

This study began with a quote by former Lockheed-Martin chief executive Norm Augustine highlighting how the costs to develop and build advanced weapons for the United States military were growing at a

---

[31] Shimko, *The Iraq Wars and America's Military Revolution*, 221; Stephen Wrage, "Prospects for Precision Air Power," 105.
[32] Gray, *Perspectives on Strategy*, 176.
[33] Additionally, Israeli efforts to develop stealth attack aircraft would be very difficult to conceal. Such efforts would almost certainly be destabilizing and may invite an attack from an adversary. These factors may contribute to Israel's reluctance to develop such stealth attack capabilities.
[34] Though the data on the costs required to develop the capability to conduct the network attacks are not available, it is highly likely they do not exceed the costs required to develop a stealthy attack aircraft.

rate faster than that of the defense budget.[35] One result of this cost growth was that the services purchase increasingly fewer of a particular platform than initially planned.[36] For instance, the Air Force purchased a total of 744 B-52s compared to only 21 B-2A bombers.[37] Similarly, a total of 867 F-15A/C aircraft were manufactured compared to only 187 operational F-22A Raptors.[38] As fewer and fewer copies of each platform are acquired, the low density of numbers is itself a vulnerability.

In *Perspectives on Strategy*, Colin Gray noted "the tactical effectiveness of weaponized technology depends not only on its technical military performance as a weapon, but also on the quantity in which it is procured. There will be a critical mass of numbers, weight of firepower and so forth, that has qualitative consequences. A few weapons in the super category of relative performance metrics are typically far less than super in tactical effectiveness when too few of them are deployed."[39]

Not only are fewer copies of individual platforms being developed, budgetary pressures are forcing the United States to purchase fewer types of weapons as well. For example, according to Lockheed-Martin, the F-35 Lightning II is being developed to replace the F-16, F/A-18, EA-6B, F-111, A-10, AV-8B, Harrier GR-7, Sea Harrier, AMX, and Tornado in American and allied inventories.[40] For an adversary whose only option is an asymmetric attack on technological vulnerabilities, the commonality

---

[35] Norman R. Augustine, *Augustine's Laws*, 6th ed (Reston, VA: American Institute of Aeronautics and Astronautics, 1997), 107.
[36] This trend is also affected by the increased capabilities of modern weapons, allowing mass and economy of force to be realized by a much smaller force.
[37] Marcelle Size Knaack, "Encyclopedia of U.S. Air Force Aircraft and Missile Systems, Volume II" (United States Air Force Office of Air Force History, 1988), 291, http://www.afhso.af.mil/shared/media/document/AFD-100526-026.pdf; United States Air Force, "B-2 Spirit Fact Sheet," April 1, 2005, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104482/b-2-spirit.aspx.
[38] Steve Davies, *F-15 Eagle and Strike Eagle* (Shrewsbury: Airlife, 2002), 90; Obaid Younossi, ed., *Ending F-22A Production: Costs and Industrial Base Implications of Alternative Options* (Santa Monica, CA: RAND, 2010), iii.
[39] Gray, *Perspectives on Strategy*, 171.
[40] "FAQs," *F-35 Lightning II*, accessed January 30, 2015, https://www.f35.com/resources/faqs.

provided by the F-35 introduces the likelihood thousands of aircraft across a multi-national coalition could be neutralized with nothing more than keystrokes. Deliberately dispersing assets geographically in an attempt to prevent their simultaneous targeting is no longer effective. The ramifications of paralyzing F-35s worldwide would almost certainly have strategic effects.

Implication 4: Self-Induced Strategic Paralysis

The preceding sections have established that America's reliance on technology has created an unknown and potentially unknowable number of vulnerabilities. The dramatic increase in the United States' combat power and effectiveness has forced its potential adversaries to seek increasingly asymmetric countermeasures.[41] Budgetary pressures have reduced the types and numbers of each weapon system procured which will likely serve to enhance the effect of a particular countermeasure. The final implication of America's reliance on technologically advanced weapon systems concerns the process required to respond to a countermeasure fielded by an adversary.

Consider once again Israel's attack on Syria. What if Syria had learned in advance of Israel's attack plans? Obviously, they would begin an effort to patch the vulnerabilities in their air defense system to ensure Israel could not attack undetected. How long would this patching process take? Would the costs involved be prohibitive?

These same types of questions matter for the United States. Dating to WWII, its adversaries have deployed countermeasures against its electronic weapon systems capitalizing on hardware and/or software vulnerabilities.[42] To maintain the combat capability and relevance of the weapon on the battlefield, the American military must do what is

---

[41] Shimko, *The Iraq Wars and America's Military Revolution*, 221.
[42] Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca: Cornell University Press, 1991), 191.

necessary to minimize the effect of adversary countermeasures. Time is of the essence in this effort.

Some of these workarounds to address an adversary countermeasure may only involve a change in tactics. However, in the extreme, the workarounds aren't as straightforward and will require modifications to weapon system hardware, software, or both.[43] Fortunately, the American defense establishment that developed the most capable military the world has ever seen will be called upon to engineer the workaround. This is both a blessing and a curse.

While the likelihood is high that a workaround exists and will be found by those charged with the task, the costs involved to field a counter-countermeasure are significant in both time and money. Due to the highly integrated nature of many of the weapon systems fielded today, any hardware or software modification is dizzyingly complex. The solutions developed must ensure other weapon system functions have not been compromised in the process of fixing the initial problem presented by the adversary's countermeasure. While this process runs its course, the American military is denied a particular combat capability. Major General Charles Dunlap calls this cycle time required to field new capabilities the "acquisition loop."[44]

The United States military is comprised of the weapon systems its planners deem are necessary to achieve effects across a broad spectrum of conflict. If an adversary deploys an effective countermeasure that prevents a particular weapon system from use in conflict, there can be strategic ramifications. Because American military strategy is so closely tied to the advanced weapons it relies on, denial of the use of those weapons while the acquisition loop cycles increases the probability of strategic paralysis.

---

[43] Gray, *Perspectives on Strategy*, 179.
[44] Charles J. Dunlap Jr., "21st-Century Land Warfare: Four Dangerous Myths," *Parameters*, Autumn 1997, 2.

As defined by David Fadok, strategic paralysis is defined as "a military option with physical, mental, and moral dimensions which intends to disable rather than to destroy the enemy. It seeks maximum possible political effect or benefit with minimum necessary military effort or cost. It aims at rapid decision through a "maneuver-battle" directed against an adversary's physical and mental capability to sustain and control its war effort to diminish its moral will to resist."[45]

America's reliance on technologically advanced weapons increases the number of ways an adversary can disable a system due to the inroads provided by hardware and software vulnerabilities. This reliance also perversely incentivizes potential adversaries to seek asymmetric countermeasures against the American military. The smaller number of aircraft in the United States military has served to enhance the effectiveness of those countermeasures. Finally, the process necessary to develop or modify complex weapon systems in response to an adversary countermeasure paradoxically jeopardizes the efficacy of the weapon itself. This idea will be explored in greater detail in the following chapter.

Conclusion

Historian John Guilmartin succinctly summarizes the problem America faces: "Are we likely to stub our high tech toes against some low tech rocks in the most miserable reaches of the Third World, or perhaps in our own backyard?"[46]

His concerns stem from the realization that technological solutions can partially alleviate social pressures to minimize the effects of conflict. Society has increasingly shied away from indiscriminate warfare. Technology has progressed to the point that society's desires can largely

---

[45] David S. Fadok, "John Boyd and John Warden: Air Power's Quest for Strategic Paralysis," 10.

[46] John F. Guilmartin, "Technology and Asymmetrics in Modern Warfare," in *Challenging the United States Symmetrically and Asymmetrically: Can America Be Defeated?*, ed. Lloyd J. Matthews (Carlisle Barracks, Pennsylvania: U.S. Army War College, 1998), 25, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB230.pdf.

be accommodated. The United States military has been the driving force behind the shift towards precision weapons. An arsenal of weapon systems brimming with computing power underpins America's military might. This carries with it four implications.

First, due to the nature of modern computers, potential adversaries can attack via any number of access points and realize effects that previously would have required the efforts of a great power. Second, the nature of American military strength invites an increasingly asymmetric threat, and also enhances the effects an asymmetric attack can realize. The American military has also fundamentally changed how it is trained and equipped based on its reliance on technology. This has translated into fewer platforms and fewer numbers of each platform. These comparatively small numbers are themselves vulnerabilities. Finally, in addressing an adversary countermeasure, technologically advanced weapon systems can be neutralized while the acquisition loop cycles.

The next chapter will begin by exploring the theoretical relevance of these implications. Then, recommendations by two Defense Science Board studies in 2009 are considered. Three additional recommendations are presented and their potential benefits are discussed. The effects of these recommendations are explored in the case studies of the F-22 in Chapter 4 and GPS in Chapter 5.

Chapter 3

Accelerating the Speed of the Acquisitions Loop

> *Although information technology is touted as a means to get inside an adversary's "decision loop," the reality is that a streetfighter or warrior nation unencumbered by Western-style procurement regulations might easily be able to get inside our "acquisition loop" and field newer weaponry well before we finish buying already obsolete equipment..*
>
> Maj Gen Charles Dunlap, USAF (Ret)

By simple virtue of its architecture, the technology the United States military relies upon is full of vulnerabilities. For those vulnerabilities that are known, protective measures either mitigate the risk, or the risk associated with the vulnerabilities has simply been accepted. Unfortunately, not all of a weapon system's vulnerabilities are known to its owner. With technology becoming increasingly complex and interconnected, the risks associated with unknown vulnerabilities has grown dramatically.

An adversary capitalizing on such vulnerabilities has the ability to "make really bad things happen." Recognizing "technology and globalization have empowered first- and second-tier states, non-states, and even individual extremists alike" with the necessary capability to do so, the Defense Science Board convened a study on capability surprise in 2009.[1] Their study assumed that surprise cannot be eliminated altogether, but can be managed.[2] The effects of such surprise are what matter, and are best understood within the context of John Boyd's Observe-Orient-Decide-Act (OODA) Loop.

---

[1] Defense Science Board, *Capability Surprise*, September 2009, vii, http://www.acq.osd.mil/dsb/reports/ADA506396.pdf.
[2] Defense Science Board, *Capability Surprise*, 29.

Colin Gray described the OODA loop as a grand theory that is elegantly simple, extensively applicable, and insightful about strategic essentials.[3] For the purposes of this study, Boyd's concepts provide a meaningful framework for understanding and addressing technologically driven vulnerabilities. Specifically, Boyd's ideas underscore the importance and relevance of the implications discussed in Chapter 2. What follows begins by describing Boyd's ideas and their relationship to the problem under consideration. The acquisition process is then outlined in broad terms to illustrate how technologically advanced weapons depend on those responsible for their development. The chapter concludes with a discussion of several measures to accelerate the speed of the acquisitions loop.

John Boyd and the OODA Loop

Nurturing ideas whose seeds were planted during the early years of his career as a fighter pilot, Air Force Colonel John Boyd devoted himself to developing a generalized theory of conflict.[4] The foundation of his theory is an iterative double-loop learning process more commonly referred to as the OODA loop.[5] The OODA loop theory is broadly applicable to behavior in general, and its explanatory power is not confined to behavior in conflict.

The first element of the process is observation, whose task is detecting "events within an individual's, or group's, environment."[6] Next, during the orientation phase, the individual or group analyses the information gathered in the observation phase and synthesizes a mental

---

[3] Colin S. Gray, *Modern Strategy* (New York: Oxford University Press, 1999), 91.
[4] David S. Fadok, "John Boyd and John Warden: Air Power's Quest for Strategic Paralysis" (School of Advanced Airpower Studies, 1995), 14.
[5] Frans P. B. Osinga, *Science, Strategy and War the Strategic Theory of John Boyd* (London; New York: Routledge, 2007), 230.
[6] Osinga, *Science, Strategy and War the Strategic Theory of John Boyd*, 230; Grant Tedrick Hammond, *The Mind of War: John Boyd and American Security* (Washington: Smithsonian Institution Press, 2001), 4.

image, which is necessarily affected by the complex "set of filters of genetic heritage, cultural predisposition, personal experience, and knowledge."[7] Decision is where individuals or groups choose between available alternatives of action created in the preceding phase.[8] Finally, actions are the implementation of the chosen decisions and serve as "validity checks on the correctness and adequacy of the existing orientation patterns."[9]

The United States military uses technology in all of the phases of its OODA loop. Therefore, an attack affecting a technological system necessarily impacts both the functioning and the outcome of the OODA loop. For instance, an attack that prevents an intelligence platform from collecting imagery affects one's ability to observe what is happening. Without this information, the orientation, decision, and action elements of the loop are impacted. This example used an attack on the observation portion of the loop, but similar consequences are realized if technologies critical to the other phases are attacked. Most concerning is the ability of an attacker to negate or degrade America's ability to *act* by attacking a technological capability.[10] Regardless of what technology is attacked or which portion of the OODA loop is impacted, the ultimate effect is determined by how the United States responds.

Recall that vulnerability has meaning at many different levels; to a policy maker it is the macro-effect of losing war-making capability while to a practitioner it is the inability to perform the designated mission. If the United States lacks the capacity to respond swiftly to a broad spectrum of attacks on its weapon systems, meso-level attacks that

---

[7] Hammond, *The Mind of War*, 4; Osinga, *Science, Strategy and War the Strategic Theory of John Boyd*, 232.
[8] Osinga, *Science, Strategy and War the Strategic Theory of John Boyd*, 232; Hammond, *The Mind of War*, 4.
[9] Osinga, *Science, Strategy and War the Strategic Theory of John Boyd*, 232; Hammond, *The Mind of War*, 5.
[10] Consider a scenario where the software of the F-35 is affected whereby the aircraft cannot perform a desired mission set. Because of the ubiquity of the aircraft and it's role in the United States arsenal, such an attack can have a disproportionate impact.

ordinarily would have only affected practitioners can have strategic, macro-level outcomes. Therefore, how the United States is able to respond to an attack contributes to the level at which an adversary's attacks are felt.

Boyd argued that the ability to iterate through the OODA loop faster than an adversary would create a situation where the foe could not react to actions effectively in time.[11] Frans Osinga states "the abstract aim of Boyd's method is to render the enemy powerless by denying him the time to mentally cope with the rapidly unfolding, and naturally uncertain, circumstances of war."[12] A nation's ability to respond flexibly would complicate the ability of such an attack to render it powerless.[13] In other words, the ability of a nation to deploy effective counter-countermeasures will determine the severity of an attack over time.[14] With today's modern weaponry, this task of developing counter-countermeasures falls to America's acquisition community.

The United States military does not maintain the capability to produce its own weapons. Instead, it procures them from civilian companies through a process designed to minimize cost, schedule, and performance risk assumed by the government.[15] Not surprisingly, the system often is lambasted for its inefficiencies and cumbersome nature. Satisfactory acquisition reform has proven to be an elusive goal dating back to the beginning of the system itself, but the requirement to procure or modify systems quickly persists.

Recognizing the import of rapidly meeting warfighter needs, the Defense Science Board commissioned another study in 2009 examining

---

[11] Gray, *Modern Strategy*, 91.
[12] Osinga, *Science, Strategy and War the Strategic Theory of John Boyd*, 237.
[13] Recall from Chapter 1 the definition of flexible response: "the capability of military forces for effective reaction to any enemy threat with actions appropriate and adaptable to the circumstances existing."
[14] This assumes that a modified tactic does not solve the problem with existing weapon configurations. If that were always the case, this study would be superfluous.
[15] LaFleur, Jeffrey, "Tear Down the Wall Chart: Rapid Acquisitions for the Rest of the Department of Defense" (Air Force Research Institute, 2012), 5.

the fulfillment of urgent operational needs. Their report stated: "The essence of the problem is the need to field militarily useful solutions faster. The reality is that the Department is not geared to acquire and field capabilities in a rapidly shifting threat environment. Current long standing business practices and regulations are poorly suited to these dynamics. Today, the Department of Defense (DoD) is saddled with processes and oversight built up over decades, and managers leading them who are often rewarded for risk aversion."[16]

Briefly, the current system involves navigating three decision-making processes simultaneously. First, the Joint Capabilities Integration and Development System (JCIDS) evaluates gaps in warfighting capabilities and develops requirements to resolve the gaps.[17] Next, the Defense Acquisition System (DAS) manages the development and procurement of weapon systems and their associated equipment.[18] Finally, the Planning, Programming, Budgeting, and Execution (PPBE) system allocates resources to fund the acquisition effort.[19] Individually, each system is labyrinthine. Collectively, the three systems create a formidable barrier to getting anything done, much less anything done quickly. Overall, the system prioritizes and places particular emphasis on fielding a 99% solution, with insufficient emphasis placed on needs that arise during the operations and support phases of a weapon system's lifetime.[20] This emphasis is illustrated by DoD Instruction 5000.02, the regulation governing the operation of the DAS.

Figure 3 below broadly depicts how the DAS approaches procurement of incrementally deployed software intensive programs, a characteristic of most modern weapon systems. The timeframe where an

[16] Defense Science Board, *Fulfillment of Urgent Operational Needs*, July 2009, viii, http://www.acq.osd.mil/dsb/reports/ADA503382.pdf.
[17] Defense Science Board, *Fulfillment of Urgent Operational Needs*, 8.
[18] Defense Science Board, *Fulfillment of Urgent Operational Needs*, 8.
[19] Defense Science Board, *Fulfillment of Urgent Operational Needs*, 8.
[20] Robert M. Gates, "A Balanced Strategy," *Foreign Affairs*, January 1, 2009, http://www.foreignaffairs.com/print/63717.

adversary would conduct an attack on a technologically advanced weapon system is far to the right, and is labeled "Operations and Support." Not only does this figure highlight the massive level of oversight involved in the development of software intensive programs, it also highlights the inability of the acquisitions program to respond to surprises during the operations and support phases.

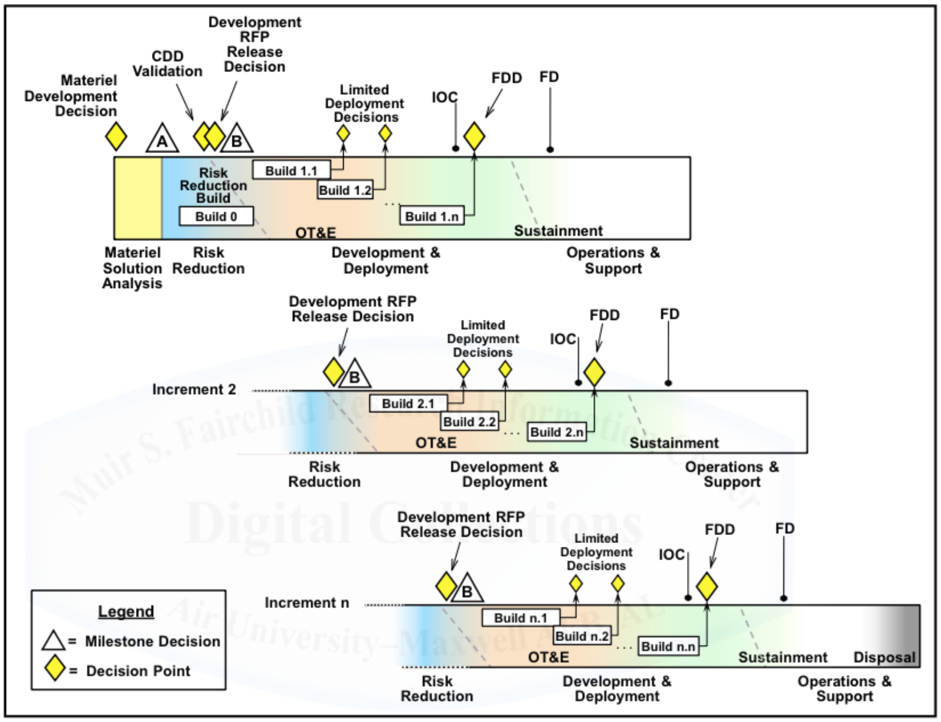

Figure 3 Incrementally Deployed Software Intensive Program
Source: DoDI 5000.02 (07 Jan 2015)

The regulation recognizes and specifically addresses the notion that programs need to be accelerated and capabilities need to be fielded rapidly. The following two figures illustrate how the DAS modifies the above timeline to more quickly field systems. Note again the lack of emphasis placed upon operations and support, and note that in Figure 5 the notional timeframes are measured in months and years.

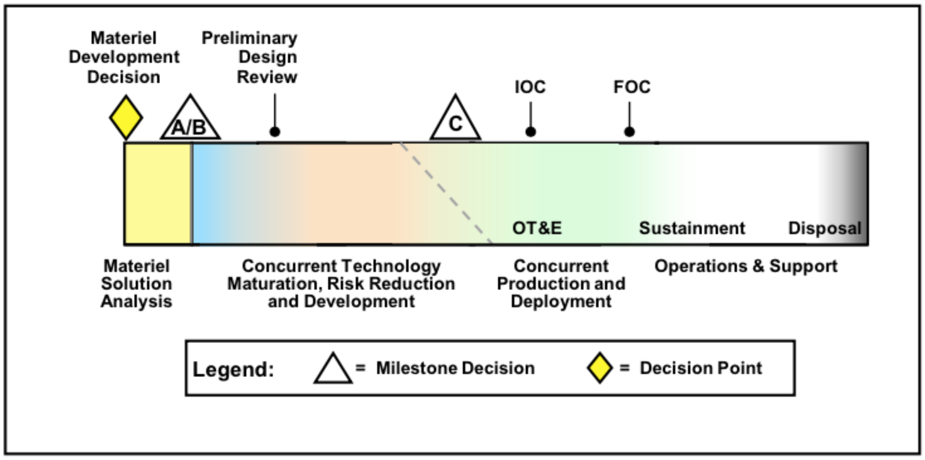

Figure 4 Accelerated Acquisition Program
Source: DoDI 5000.02 (07 Jan 2015)

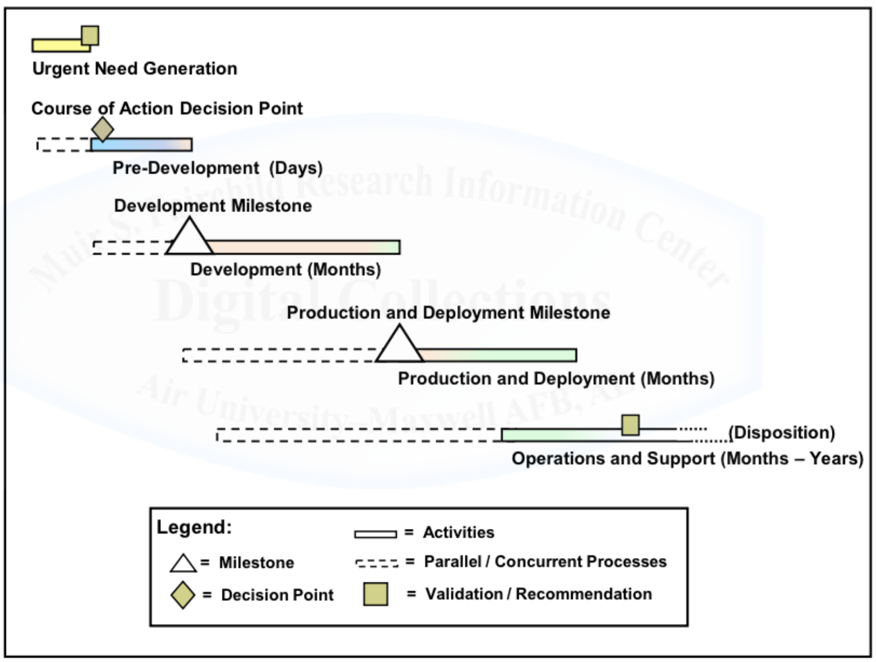

Figure 5 Rapid Fielding of Capabilities
Source: DoDI 5000.02 (07 Jan 2015)

Undoubtedly, any foray into the DAS is going to be arduous. The system is neither built for speed nor agility, and any expectation of a quick and effective outcome is misguided. Unfortunately, it is this same system that supports our ability to iterate through the OODA loop faster than our adversary, whose ultimate aim is to render us powerless.

As discussed in Chapter 2, the growing dependence of modern weapon systems on technology increases their vulnerability as well as the associated risk assumed by strategists. When a vulnerability is exploited, the development of the counter-countermeasure will almost assuredly involve the acquisition community and rely upon a system woefully ill-prepared for such a task. While the acquisitions loop cycles, the overall OODA loop is compromised. This phenomenon continues until the counter-countermeasure is fielded further emphasizing how the overall OODA loop is becoming *increasingly reliant upon* on the acquisition loop.[21] Therefore, to minimize the overall vulnerability of a system, the speed of the acquisitions loop must be accelerated.

Maximizing the Speed of the Acquisition Loop

The following discussion considers improvements aimed at maximizing the speed of the acquisitions loop. However, this study should not be confused as yet another plea for acquisitions reform writ large.[22] It instead identifies the link between technology and risk, and describes how the speed of the acquisitions loop unnecessarily accentuates system vulnerabilities. Improving the speed of the acquisitions loop can decrease overall risk across the entire United States military inventory.

Significant scholarship on how to improve the acquisition system exists, and warrants consideration. Therefore, the recommendations of the two aforementioned Defense Science Board studies are briefly summarized. They are followed by additional measures that can help to ensure the effects of an adversary's attack are not accentuated by an acquisitions community incapable of developing a sufficient counter-countermeasure.

---

[21] Indeed, there are other "loops" that matter to the overall OODA cycle. Inefficiencies in training or logistics can also have similar deleterious effects like those being considered in this study.

[22] Reform still needs to happen, but is well beyond the scope of this study.

The Defense Science Board made the following four recommendations in their 2009 study on Capability Surprise:

1. Establish a Capability Assessment, Warning, and Response Office (CAWRO) to provide DoD senior leadership with timely assessment and warning of potentially high-risk adversary capabilities, with options for addressing them.

2. Red team to address strategic level issues, and as part of major acquisitions, exercises, and developmental education.

3. Establish a standing Rapid Capability Fielding Office (RCFO) to improve DoD capabilities for addressing priority surprise capability gaps and supporting urgent war fighter needs.

4. Improve strategic intelligence to provide insight into adversary capabilities, intent, vulnerabilities, and denial and deception efforts.[23]

Five recommendations were made in the Defense Science Board's 2009 report on the Fulfillment of Urgent Operational Needs. They are:

1. The Secretary of Defense should formalize a dual acquisition path. (See Figure 6)

[23] Defense Science Board, *Capability Surprise*, xiv–xv.

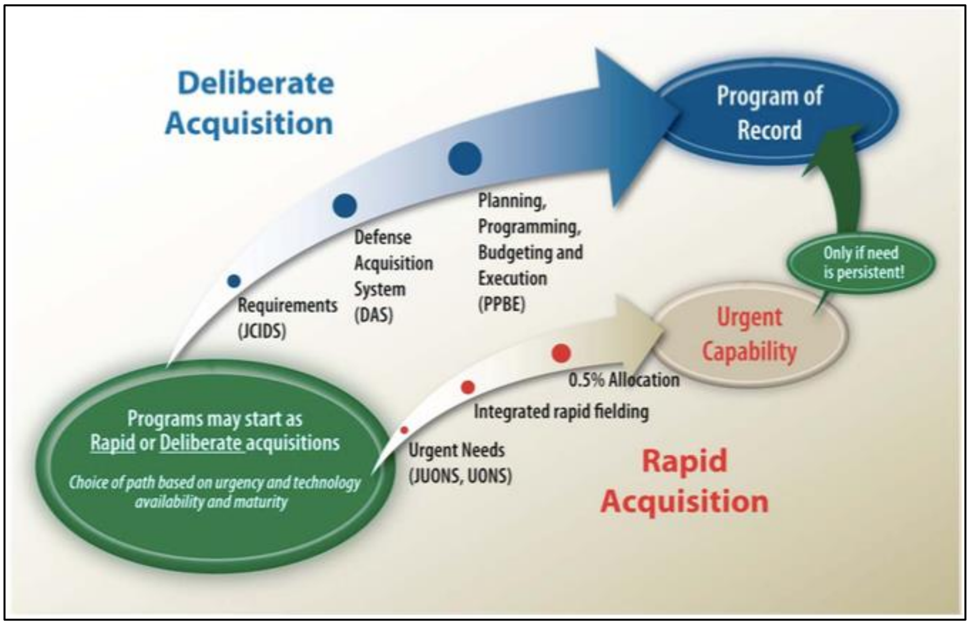

Figure 6 Defense Science Board Dual Acquisition Path Concept
Source: Defense Science Board Fulfillment of Urgent Operational Needs

2. Executive and Legislative branches must establish a fund for rapid acquisition and fielding.

3. The Secretary of Defense should establish a new agency with a proposed name of Rapid Acquisition and Fielding Agency (RAFA). The agency will be "focused on speed, utilizing existing technologies, and acquisition flexibilities to achieve a 75 percent solution initially 'good enough' to address the urgent needs of the warfighter."

4. Initial billets and funding for RAFA will be based on absorbing and integrating existing programs and organizations.

5. DoD should establish a streamlined, integrated approach for rapid acquisition.[24]

Adopting the recommendations from either or both studies would indeed accelerate the speed of America's overall acquisition loop. The panels both identified and recommended creating pathways to circumvent the crippling bureaucracy of the traditional acquisition

[24] Defense Science Board, *Fulfillment of Urgent Operational Needs*, x–xii.

processes. However, they fail to acknowledge explicitly the very real possibility that a weapon system may be crippled until a viable counter-countermeasure is fielded.

For that reason, this study recommends three additional measures beyond those proposed by the two Defense Science Board studies. First, a viable development capability must be kept in "warm" status throughout the life of a technologically advanced weapon system. Next, alternative contractual requirements should be considered to ensure the acquisition loop can cycle as fast as possible. Finally, pursuing nearly perfect solutions significantly slows the speed of the acquisitions loop. Reintroducing the concept of 'good enough' will dramatically improve the speed of the acquisitions loop. Each of these additional recommendations is explored in greater detail below.

Recommendation #1: Warm Status

When capability surprise occurs, the United States military will understandably seek to restore the capability of the affected weapon system as soon as possible. This effort will almost certainly involve working with the company that developed the weapon system. Because of the decades-long lifespans of modern weapon systems, there is a good chance that much of the corporate knowledge that initially designed the attacked system has departed the company. In this type of a scenario, engineers at the company will be required to do research to understand the fielded system enough to develop the counter-countermeasure. This research period adversely affects the speed of the company's response and slows the speed of the acquisition loop.

The uncertainty and delays associated with this research period can be minimized by requiring the contractor to maintain a team of engineers for developing rapid fixes to attacks on weapon systems. This team would participate in regular exercises, where fictitious attacks would occur and require the team to devise solutions to the notional problems created.[25] This concept is closely related to the second recommendation made by the Defense Science Board Capability Surprise study, which highlighted the benefits of red teaming. Maintaining a team of engineers in "warm status" goes a step further and ensures that the contingency has been considered and a solution is developed.[26] A potential venue for this construct would be to identify a countermeasure at the beginning of a Red Flag and attempt to field a viable counter-countermeasure by the end of the exercise. This construct yields all the benefits of the red teaming efforts that identify vulnerabilities.[27] It also maximizes the speed of the acquisition loop because it benefits from the many lessons learned in the exercises. Additionally, such events will almost certainly improve the overall capability of the system. At the very least, they will develop capabilities and expertise that can be critical when capability surprise occurs. These experiences will be critical in identifying and eliminating bottlenecks that unnecessarily slow the acquisition loop.

Recommendation #2: Alternative Contractual Requirements

The speed of the acquisitions loop can be increased if creative alternative contractual arrangements are established between defense contractors and the government. Two such requirements warrant consideration. The first involves transparency regarding contractor research efforts while the second involves how easy or difficult it is to modify or upgrade a weapon system.

---

[25] The problems presented in these exercises would ideally be threat-representative so as to further enhance the military's readiness.
[26] Red teams generally identify problems or capability gaps. Rarely are they staffed with sufficient expertise or resourced to assist in developing solutions to the problems they've identified. The proposed construct removes this limitation characteristic of red teams.
[27] Singer and Friedman, *Cybersecurity and Cyberwar*, 114–120; Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Do About It*, 1st Ecco pbk. ed (New York: Ecco, 2012), 211–213.

Defense contractors conduct research, development, test and evaluation (RDT&E) efforts on new technologies to either enhance existing weapon systems, fix documented or undocumented deficiencies, or as part of future development projects. Often times, the company initiates and funds these efforts independent of government contracts in what are known as independent research and development, or IRAD, efforts. Their hope is that the finished IRAD product eventually attracts a contract after the contractor pitches the new capability to the government. Until that happens, the products of these IRAD efforts often live “on the shelf” without government knowledge of the capabilities they bring.

This information asymmetry alters how the military responds to an attack on a weapon system. After an attack occurs, the military observes its effects. Next in the OODA loop are the orientation and decision phases, which are framed by existing knowledge bases and an awareness of available options. Because the contractor has a monopoly on the knowledge of what options are available, the military’s ability to make fully informed decisions is marginalized.

Therefore, contractors for fielded weapon systems should be required to disclose results of IRAD concerning fielded weapon systems, to include any enhancements or deficiency fixes that are available. Any information provided to the government concerning new capabilities will be protected just like any other proprietary information. The additional transparency provided by this disclosure requirement will serve to increase the speed of the acquisition loop by allowing the military to make fully informed decisions when capability surprise occurs.

A second contractual requirement worth considering is the establishment of a performance parameter requirement that is tied to the speed at which a weapon system can be modified. Similar requirements already exist for currently fielded weapon systems. For instance, an aircraft may have a requirement to be available to the warfighter for a particular percentage of time. This requirement ordinarily incorporates the expected mean time between failures and the expected maintenance action times.[28] In effect, this requirement drives how easy or difficult it is to repair the system. It also factors into how the system is designed up front, balancing how robust the system is with how easy it is to fix it. Such a requirement for the computing hardware on weapon systems will permeate the development stages for new systems, enabling more rapid fielding of counter-countermeasures.

Recommendation #3: What's Good Enough?

The issue of what constitutes a sufficient counter-countermeasure looms as each of these options are considered. Historically, the military has sought near-perfect systems to minimize the risk of having to pay for future modifications of the system. This approach should be abandoned in favor of acknowledging that systems will continuously evolve throughout their life cycles. Dan Ward, a former Air Force acquisitions officer, recommends future "projects advance through an iterative series of incremental steps, each of which provides a portion of the required capability and establishes a foundation for adding future capabilities as needs emerge and are validated."[29]

This new approach will re-introduce "good enough" into the military vernacular and will dramatically improve the speed of the acquisition loop. Robert Gates, writing in *Foreign Affairs* as the Secretary of Defense, supported a similar approach for stability and counterinsurgency missions: "The Department of Defense's conventional modernization programs seek a 99 percent solution over a period of

---

[28] Defense Acquisitions University, "Defense Manufacturing Management Guide for Program Managers, Chapter 5.6 Reliability, Availability, and Maintainability" (Defense Acquisitions University, July 5, 2012), https://acc.dau.mil/communitybrowser.aspx?id=520790.

[29] Dan Ward, *F.I.R.E.: How Fast, Inexpensive, Restrained, and Elegant Methods Ignite Innovation*, First edition (New York: Harper Business, 2014), 18.

years. Stability and counterinsurgency missions require 75 percent solutions over a period of months."[30]

Unfortunately, there will be circumstances where a successful counter-countermeasure is an either-or proposition. Sometimes, there won't be a 75 percent solution; it either works or it doesn't. For those instances, incorporating the recommendations made by the Defense Science Board and the other ideas presented above will accelerate the speed of the acquisition loop and facilitate fielding the functioning counter-countermeasure more quickly.

The Way Forward

The discussion above considers technologically advanced weapon systems that have already been fielded and the complications associated with responding to an attack. Some of the vulnerabilities and complications are self-inflicted, and are products of how the systems were developed in the first place. New ways of thinking about system development suggest that the system architecture itself can assist in fielding effective counter-countermeasures quickly. For systems still in their design phase, incorporation of these architectures will enhance the system's resilience and decrease risk.

Modifications are simplified when a system is modularly designed from the start with well-designed interfaces in an open architecture.[31] These attributes ensure systems can be modified with confidence that the changes will not adversely affect other system attributes.[32] More importantly, it ensures multiple vendors will be attracted toward supporting a given platform, providing additional options for fielding

---

[30] Gates, "A Balanced Strategy."
[31] Ward, *F.I.R.E.*, 22; Dr. Camron Gorguinpour, Director of Transformational Innovation, Telephone, February 26, 2015.
[32] Dr. Camron Gorguinpour, Director of Transformational Innovation; Chris Gentile, United States Air Force Rapid Capabilities Office Program Manager, Telephone, February 26, 2015.

improvements to a system after an attack.[33] In short, these system characteristics increase the adaptability of the system over the long term.[34]

Another concept to consider is technology that autonomously adapts to its environment. Historically, this idea has been reserved for science fiction. However, today's technology makes it a realistic possibility. Specifically applied to this study, an advantage of artificially intelligent systems is that they would not need to be modified or repaired to respond to a countermeasure.[35] The logic for the adaptation would be baked in from the start, effectively eliminating the speed of the acquisitions loop as a critical factor.

Conclusion

This study argues the pervasiveness of technology in the United States' military inventory creates strategic vulnerability. The ability to deliver new capabilities rapidly is itself a strategic capability.[36] Using Colonel John Boyd's OODA loop as an analytical framework, this chapter examined the relationship between the acquisitions and operations communities in fielding counter-countermeasures in response to an adversary attack affecting America's technological capability. The speed of the acquisitions loop is critical to maintaining the function of the overall OODA loop. This can be accomplished via adoption of several recommendations proposed by the two Defense Science Board studies in 2009. The speed of the acquisitions loop can be further accelerated by maintaining engineering expertise in warm status, implementing alternative contractual requirements defense contractors must meet, and

---

33 Dr. Camron Gorguinpour, Director of Transformational Innovation.
34 Ward, *F.I.R.E.*, 22.
35 P. W Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century* (New York: Penguin Books, 2010), 74–75.
36 Ward, *F.I.R.E.*, 20.

by accepting solutions that are ‘good enough’ to meet time-critical challenges.

The next chapter uses the recommendations just presented and considers how they would benefit the F-22 in its ability to respond to an adversary attack. The chapter begins with a brief discussion of why the F-22 was chosen as a case study and why its challenges are emblematic of trends in other modern weapon systems. The F-22’s system engineering process is then described to establish a baseline for how quickly its acquisitions loop can run. Then, several recommendations are applied to help illustrate how they can improve the performance of the F-22’s acquisitions loop.

Chapter 4

Case Study #1: The F-22 Raptor

The essence of the problem is the need to field militarily useful solutions faster. The reality is that the Department is not geared to acquire and field capabilities in a rapidly shifting threat environment. Current long standing business practices and regulations are poorly suited to these dynamics. Today, the DOD is saddled with processes and oversight built up over decades, and managers leading them who are often rewarded for risk aversion.

Defense Science Board
Report on The Fulfillment of Urgent Operational Needs

Intended to replace the F-15C Eagle as America's air dominance platform, concept definition for the F-22 Raptor occurred in November 1981.[1] The aircraft reached initial operating capability on December 15, 2005, and the Air Force declared it fully operational on December 12, 2007.[2] The Raptor was the world's first fifth generation fighter, and represented a dramatic increase in capability over earlier generation aircraft in a number of areas.[3] Among these capability increases was the level of integration designers built into the aircraft's sensors, controls, systems, and displays.[4] To achieve such integration, designers leveraged advances in computing technology, with virtually no F-22 system able to function independent of electronic computers.[5] While this served as a key enabler for many of the Raptor's advanced capabilities, it also introduced a number of vulnerabilities to which previous generations of fighter aircraft were not as susceptible.

---

[1] Aronstein, Hirschberg, and Piccirillo, *Advanced Tactical Fighter to F-22 Raptor Origins of The 21st Century Air Dominance Fighter*, 1.
[2] Younossi, *Ending F-22A Production*, 2.
[3] Younossi, *Ending F-22A Production*, 1.
[4] Aronstein, Hirschberg, and Piccirillo, *Advanced Tactical Fighter to F-22 Raptor Origins of The 21st Century Air Dominance Fighter*, 1, 171.
[5] Aronstein, Hirschberg, and Piccirillo, *Advanced Tactical Fighter to F-22 Raptor Origins of The 21st Century Air Dominance Fighter*, 171–179.

Just like any weapon system, the F-22 continues to develop and evolve even after fielding. Over time, certain situations will demand that its systems receive upgrades or modifications to maintain functionality, relevance, and capability advantage over potential adversaries. The discussion that follows broadly describes the process used to field the upgrades or modifications. This process is then evaluated against the framework presented in the preceding chapter. The complexity of the process underscores the arguments made previously: inefficiencies in the acquisition loop create critical vulnerabilities whose effects can be significant or even prove to be decisive.[6]

The F-22 serves as a case study because its architecture and reliance on technology is representative of trends in modern weaponry. General conclusions concerning its relationship to the acquisition loop are applicable to other modern aircraft systems, such as the B-2, F-35, and the next generation bomber. The general conclusions also apply to weapons used by other services in other domains. This case study highlights vulnerabilities rooted in technology whose first order effects only impact a single platform. In other words, adversary actions necessitating an upgrade or modification to the F-22 would not simultaneously have similar effects on another platform.

Before delving into the process used by the F-22 program to upgrade or modify the aircraft, an example is presented to show the effects of the acquisition cycle on the warfighter. It illustrates how a seemingly inconsequential change to the F-22's software can impose millions of dollars in cost and months of work prior to fielding. While this scenario was not necessarily responding to capability surprise or filling an urgent operational need, the lessons it carries are transferable to such situations.

[6] See Chapter 1 for a more comprehensive treatment of what constitutes a critical vulnerability.

A modernization effort that had been planned for the F-22 completed its developmental and operational test programs and was subsequently approved for fielding by the program office. According to Charles Staley, former chief engineer and current Deputy Director of the F-22 Combined Test Force, as operational units installed the new software, they noted certain weapon systems capabilities, both old and new, were not functioning properly.[7] Though this is exactly the scenario the test process is designed to avoid, it happened. Ultimately, the culprit was identified. The F-22 software expected a particular chip's output to have very tight tolerances. However, the production specifications for the chip's output were not as narrow as the software expected them to be.[8] The software performed well on the test aircraft whose output happened to be within these expectations. Once it was installed on several operational aircraft with a wider range of chip outputs, the software failed to perform properly.[9]

Fixing the situation required the development and testing of an entirely new software load. From the time the operational units identified the problem to fielding a new solution took three months.[10] The fix increased the cost of the modernization effort by approximately $7 million dollars.[11] Significantly, the added time and additional money required provided no additional capability to the aircraft and delayed other planned modernization efforts by occupying the F-22 engineering and test enterprises.

This vignette exemplifies the argument made in Chapter 2 that technologically advanced weapons are subject to known and unknown vulnerabilities. This situation is unique in that it was self-induced and not a result of adversary actions. However, the end result is the same.

[7] Charles Staley, Personal communication, January 9, 2015.
[8] Charles Staley, Personal communication.
[9] Charles Staley, Personal communication.
[10] Charles Staley, Personal communication.
[11] Charles Staley, Personal communication.

Adversary actions can similarly trap the United States in a recurring acquisitions loop, thereby denying us the use of a particular capability or platform.[12]

Why was this process so cumbersome? To answer that question requires an understanding of the systems engineering process used by the F-22 program. While the steps involved are there for good reason, they all but eliminate the possibility of fielding rapidly any sort of capability on the aircraft involving a change to the computing hardware or software.

Upgrading or Modifying the F-22

After fielding a weapon system, astute militaries will continue to evaluate the efficacy and relevance of the system on the battlefield. Generally speaking, one of two reasons compels a military to upgrade or modify a particular weapon system outside of normal modernization schedules. The first results from an organic evaluation of the weapon system where a deficiency is identified either in test or training operations. In this scenario, the adversary capability remains constant. The second path responds to actions taken by a potential adversary, where the adversary capabilities change. These adversary actions can include fielding a countermeasure in the form of a new weapon system, modifying an existing weapon system, or simply updating existing tactics, techniques, and procedures.[13]

For the purposes of this discussion, either pathway will similarly stimulate the acquisition loop. Either will mandate that the F-22 be upgraded or modified to maintain full capability on the battlefield. The systems engineering process for developing the upgrade or modification

[12] Admittedly, another option is available to combatant commanders who can choose to conduct operations prior to fielding necessary counter-countermeasures. However, this course of action can significantly elevate the risk assumed because the vulnerabilities have not been addressed.
[13] Defense Science Board, *Capability Surprise*, September 2009, vii-viii, http://www.acq.osd.mil/dsb/reports/ADA506396.pdf.

is structured identically for small and big software changes alike. For the F-22, it is a one-size-fits-all approach.[14] The following discussion considers modifying or upgrading only the F-22 software, as upgrades involving hardware modifications only add complexity. This highlights what should be the fastest running acquisitions loop for the F-22 is slow and cumbersome.

F-22 Systems Engineering

Upon identifying a requirement to modify the aircraft software, the program office (responsible for managing the weapon system throughout its lifetime) will ensure a contractual vehicle is in place with the contractor to perform the engineering to develop and field the upgrade.[15] During this period, contracting officials and legal teams negotiate the terms of the contract while engineering teams determine the technical requirements to be met.[16] Each of these negotiation processes are prerequisites for work to begin on the upgrade or modification, and are riddled with disparate interests. If a contract is already in place, some or all of this negotiation process may be bypassed. In the event no contract is in place, these negotiations can delay fielding by weeks or months.[17]

---

[14] Surprisingly, the systems engineering process in place is *not* something mandated by Joint Service Specification Guides or MIL-HDBK guidance (which replaced the MIL-STD). Instead, these processes are designed by the contractor and are tailored to suit each program. The benefit of this construct is that the systems engineering process for a particular platform isn't saddled with requirements intended for another platform. However, one significant drawback is that because the contractors design the processes, they are more likely to be excessively risk-averse. This translates into a process that slows down the speed of the acquisitions loop.
[15] J. Ronald Fox, *Defense Acquisition Reform, 1960-2009; An Elusive Goal* (Washington, D.C: Center of Military History, 2011), 10.
[16] The engineering teams referenced here could be located at the program office, a lab, or at a developmental or operational test organization. Both the first or second pathways described at the beginning of this chapter require some level of analysis to determine the insufficiency of the existing configuration of the weapon system. The same entity likely will be involved in determining technical requirements the upgrade or modification must satisfy.
[17] Robert E. McShea, *Test and Evaluation of Aircraft Avionics and Weapon Systems*, AIAA Education Series (Raleigh, NC : Reston, Va: SciTech Publishing ; American Institute of Aeronautics and Astronautics, 2010), 12.

Once work can begin, the team assigned to develop a solution begins by analyzing the available data regarding the issue. In the early stages of this type of effort, there will be a relatively small number of specialists involved. As the upgrade or modification begins to mature, this number grows, though many are involved to simply verify that other systems were not adversely affected by the upgrade. When the designated engineering teams are confident the upgrade or modification fixes the immediate issue, the software has reached what is called Equipment Operational Flight Certification (EOFC) Level 1.[18] This allows release of the software to evaluate performance in a laboratory setting.[19] For instance, consider a modification to minimize the effect of a new adversary jamming technique. Lab testing at EOFC Level 1 would test the modification in a lab and not on hardware that is flight qualified.

At the next stage of maturity, EOFC Level 2, the software is released for installation on an F-22 equipped with test instrumentation for limited ground testing.[20] In our hypothetical radar upgrade, testing at this level would involve a limited evaluation of the functionality of the software on flight-qualified hardware. The testing accomplished at this stage accounts for differences in hardware between the laboratory environment and actual flight hardware installed on the aircraft. To minimize risk, the aircraft is on the ground and the testing also involves diagnostic monitoring equipment to assist in troubleshooting unforeseen problems that may arise.[21] The software is then released for non-flight ground tests at EOFC Level 3.[22] This testing is accomplished without

[18] Phil Damon, "F-22 Joint Procedure 035: Operational and Flight Clearance Approval and Documentation," July 3, 2014, 7.
[19] Phil Damon, "F-22 Joint Procedure 035: Operational and Flight Clearance Approval and Documentation," 7.
[20] Phil Damon, "F-22 Joint Procedure 035: Operational and Flight Clearance Approval and Documentation," 7.
[21] Phil Damon, "F-22 Joint Procedure 035: Operational and Flight Clearance Approval and Documentation," 7–8.
[22] Phil Damon, "F-22 Joint Procedure 035: Operational and Flight Clearance Approval and Documentation," 7–8.

diagnostic equipment that was used at EOFC Level 2 to monitor inputs and outputs to the systems during test.[23] Notionally, the presence of diagnostic equipment monitoring the test should not affect the test results. Therefore, one can reasonably expect that successfully completing EOFC Level 2 testing bodes well for what is required at EOFC Level 3.

Finally, if the ground tests results are satisfactory, the software is declared to be EOFC Level 4, allowing flight test to begin.[24] As with EOFC 2, certain testing must first be accomplished to ensure that the modification doesn't affect systems required for safety of flight. Upon determination that the software is safe, the upgrade or modification can proceeds for testing at EOFC Level 5.[25]

This level of testing is the most realistic and the most relevant because it most closely simulates the actual conditions the weapon system will encounter in combat.[26] If the software is successful in meeting the specifications and has military utility, it is released to the fielded forces for full installation and use.[27]

The above process sounds very straightforward, and in theory it is. However, in practice it operates in a resource-constrained environment and attempts to serve many different interests. These two factors combine to complicate the ability of the acquisitions loop to run as smoothly as possible, with the minimum time to cycle through the loop on the order of months. To illustrate the efficacy of the recommendations made in Chapter 3 on accelerating the speed of the acquisitions loop, it is

---

[23] Phil Damon, "F-22 Joint Procedure 035: Operational and Flight Clearance Approval and Documentation," 7–8.
[24] Phil Damon, "F-22 Joint Procedure 035: Operational and Flight Clearance Approval and Documentation," 8.
[25] Phil Damon, "F-22 Joint Procedure 035: Operational and Flight Clearance Approval and Documentation," 8.
[26] McShea, *Test and Evaluation of Aircraft Avionics and Weapon Systems*, 6–7.
[27] Phil Damon, "F-22 Joint Procedure 035: Operational and Flight Clearance Approval and Documentation," 8.

useful to consider generalized contingencies common to weapon systems after they've been fielded.

No Plan Survives First Contact

The following three contingencies are representative of issues that have plagued the acquisitions community in the past and will continue to do so in the future in responding to capability surprise or to fill an urgent operational need. They are not specific to the F-22; rather, they affect virtually every fielded weapon system to include the F-22. What follows illustrates both the challenges associated with operating in the current paradigm and the benefits afforded by the recommendations made in Chapter 3. The first challenge highlights how the current system creates resource constraints that affect the speed of the acquisitions loop in the near and long-term. The second challenge highlights how a lack of engineering expertise can slow the acquisitions loop to a halt. Finally, the effects of limited test assets and multiple configurations on the speed of the acquisitions loop are discussed.

Insufficient Resources to Fund The Effort

A program manager faced with a new requirement to field an effective counter-countermeasure is in a precarious financial situation. The program probably does not have sufficient resources for what's already planned, and this new requirement upends those plans. For a number of reasons, programs regularly find themselves in a situation where circumstances demand a timely and effective upgrade or modification be fielded, but the program is rarely allocated additional resources with which to accomplish the task.[28] Ultimately, tradeoffs in cost, schedule, and performance will determine the chosen upgrade or

[28] The reasons alluded to here are beyond the scope of this study. Suffice it to say, programs seek first to solve these types of problems with available resources because of the low likelihood of getting a resource stream in a timely fashion.

modification, and will almost certainly disrupt existing modernization plans due to the redirection of resources towards the effort to solve the immediate problem.

The Defense Science Board recommended a separate funding stream for rapid acquisitions and fielding.[29] While those resources would likely be insufficient alone to satisfy the requirements of all urgent operational needs across the DoD, they would improve the current construct in two important ways. First, the funding stream would allow work to begin almost immediately on necessary upgrades and modifications while more specific funding vehicles are negotiated and established, directly improving the speed of the acquisitions loop. Second, it would also dampen the long-term effects this scenario has on planned modernization efforts. By stabilizing those moving targets, the costs associated with the long-term efforts would likely decrease as well.

The Board also recommended establishing a standing rapid capabilities fielding office in addition to a second acquisitions path to address capability surprises that generate urgent operational needs.[30] These alternate avenues would serve to insulate the existing acquisitions path focused on long-term modernization efforts from the effects of capability surprise, enhancing the overall efficiency and effectiveness of both efforts. Additionally, these rapid acquisition mechanisms would likely be streamlined to ensure that capabilities reach the warfighter more quickly than the existing system can generate, again accelerating the speed of the acquisitions loop.

Dearth of Engineering Expertise

As weapon systems reach full operational capability, the number of people involved in the program decreases. No longer is there an

---

[29] Defense Science Board, *Fulfillment of Urgent Operational Needs*, July 2009, x, http://www.acq.osd.mil/dsb/reports/ADA503382.pdf.
[30] Defense Science Board, *Capability Surprise*, xv; Defense Science Board, *Fulfillment of Urgent Operational Needs*, x.

enormous engineering footprint at the factory writing and modifying new code. Instead, what personnel remain are dedicated to modernization programs that have been years or decades in the making. Cost conscious managers at the contractors ensure that only the necessary disciplines are represented, thus avoiding paying for engineering expertise not directly supporting the modernization effort.

Unfortunately, adversary actions that necessitate the rapid fielding of an upgrade or modification are not attentive to the engineering expertise on hand. Therefore, the potential exists for a platform to require a capability that the on-hand engineering team is not suited to develop. In such a situation, the contractor will have to locate, screen, and familiarize a team to develop a solution to the problem. Each of these steps is rife with individual constraints and associated delays. In this type of situation, the acquisition loop can grind to a halt.

The preceding chapter highlighted the value of red teaming that was suggested by the Defense Science Board study on capability surprise. Building on the value of red teaming, a further suggestion was made to contractually require companies to maintain sufficient engineering expertise on hand in a warm status throughout the life span of a weapon system to meet the demands of capability surprise. This team would periodically participate in red teaming exercises where upgrades or modifications would be generated for a particular platform. The team would do more than simply go through the motions. The red teaming exercises would actually produce new capabilities that would be fielded, thereby exercising the entirety of the process. Doing so would serve to validate the expected performance of the acquisition loop, and would also provide added capability to the platform in question.

These red teaming efforts can also help to support two other recommendations made by the Defense Science Board to address capability surprise. First, the board recommended the creation of a Capability Assessment, Warning, and Response Office (CAWRO) to provide DoD senior leadership timely assessment and warning of potentially high-risk adversary capabilities, with options for addressing them.[31] Red team efforts can assist this office in quantifying the effects of adversary capabilities as well as working to develop solutions to address these gaps. As envisioned by the Defense Science Board, the office could quickly devolve into 'Chicken Little,' highlighting a growing threat but not empowered to do anything about it. Incorporating a red team with sufficient engineering backbone into the construct helps to enhance the utility of this office from identifying solutions to being an integral part of developing quick and effective solutions addressing nascent adversary capabilities. Integrating these two functions will accelerate the speed of the acquisitions loop.

The proposed requirement that contractors disclose independent research and development (IRAD) to the government also contributes to the spirit of the Defense Science Board's recommendation to establish a CAWRO. Specifically, the office is tasked to provide options to senior DoD leadership for addressing adversary capabilities.[32] Understanding what capabilities the contractor already has developed will ensure senior leaders have a clear picture of what is available on the shelf. Eliminating the time required to develop a new capability dramatically accelerates the speed of the acquisitions loop.

The second Defense Science Board recommendation was to improve strategic intelligence to provide insight into adversary capabilities, intent, vulnerabilities, and denial and deception efforts.[33] This recommendation fits nicely with the recommendation to establish the CAWRO and develop red teaming capabilities. For the CAWRO to provide meaningful inputs to senior DOD leadership, it requires high fidelity strategic intelligence, defined by Joint Publication 1-02 as

---

[31] Defense Science Board, *Capability Surprise*, xiv.
[32] Defense Science Board, *Capability Surprise*, xiv.
[33] Defense Science Board, *Capability Surprise*, xv.

"intelligence required for the formation of policy and military plans at national and international levels."[34] Additionally, for the red team to address issues of import to the CAWRO and relevant to the war fighter, it too needs high fidelity strategic intelligence.

Finally, the close relationship between the contractor red team and the CAWRO will help identify when a counter-countermeasure is sufficient for fielding. Historically, upgrades or modifications are matured until they are near perfect solutions to a given problem. Sometimes imperfect solutions can be fielded to satisfy immediate needs while the contractor's engineering team refines the solution.

Test Assets Not Properly Configured to Support

The F-22 production line ran from 1997 to 2012.[35] Over that timespan, computing technology matured and the aircraft built at the end of the program had different hardware than those built at the beginning of the program.[36] Upgrading an aircraft to the latest configuration is an involved months-long maintenance effort. Additionally, resource limitations forced the program to decide not to upgrade the oldest aircraft used for initial F-22 training to the same hardware configuration as those in the combat coded squadrons.[37] These factors translated into fragmentation of the fleet's configuration, with many different configurations of the aircraft fielded at any given time.[38]

---

[34] "Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms," November 14, 2014, 237, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
[35] Younossi, *Ending F-22A Production*, 2; Lockheed Martin, "Lockheed Martin Delivers Final, Historic F-22 Raptor to U.S. Air Force," *Lockheed Martin Press Release*, May 2, 2012, http://www.lockheedmartin.com/us/news/press-releases/2012/may/120502ae_final-f-22-delivered.html.
[36] Jeremiah Gertler, *Air Force F-22 Fighter Program: Background and Issues for Congress* (Washington, D.C.: Congressional Research Service, December 22, 2009), 13, http://www.au.af.mil/au/awc/awcgate/crs/rl31673.pdf.
[37] Jeremiah Gertler, *Air Force F-22 Fighter Program: Background and Issues for Congress*, 13.
[38] Jeremiah Gertler, *Air Force F-22 Fighter Program: Background and Issues for Congress*, 13.

Modernization schedules may dictate that the test assets be configured a particular way to support planned upgrades on either newer or older hardware configurations. With limited test assets, the possibility exists that an upgrade to a particular configuration cannot be evaluated without first modifying the test aircraft. This complicates the ability of an enterprise seeking to posture itself to respond quickly to capability surprise or to field a capability to meet an urgent operational need.

The Defense Science Board Capability Surprise report recommended establishing the CAWRO and Rapid Capability Fielding Office (RCFO) to provide "DOD leadership timely assessment and warning of potentially high-risk adversary capabilities with options for addressing them" as well as "improving DOD capabilities for addressing priority surprise capability gaps and supporting urgent war fighter needs."[39] Each of these relies on a robust strategic intelligence backbone, which is another recommendation of the board's study.[40]

In an effort to accelerate the speed potential of the acquisitions loop, these offices would work closely with the F-22 program office to ensure that test assets are configured such that they can be gainfully employed in developing rapid upgrades or modifications to the platform.

Conclusion

The F-22 Raptor is a highly advanced weapon system, though many of its capabilities depend upon computing technologies with unavoidable inherent vulnerabilities. The above case study illustrates how cumbersome the systems engineering process is to upgrade or modify the F-22, with a recent problem requiring a three-month and approximately $7 million dollar fix. Were this process responding to adversary actions taken capitalizing on the systems vulnerabilities instead of a self-induced error, the possibility exists that the United

[39] Defense Science Board, *Capability Surprise*, xiv–xv.
[40] Defense Science Board, *Capability Surprise*, xv.

States Air Force could not provide air superiority, a doctrinal core function, while the acquisition loop cycled for three months.[41]

Undoubtedly, the speed of the acquisitions loop is currently insufficient to respond to capability surprise or to fill warfighter urgent operational needs. The recommendations made in the previous chapter were applied to the F-22 program to illustrate the benefits they offer. While they will almost certainly have inefficiencies of their own, their implementation will accelerate the acquisitions loop and enhance the flexible response capability of the United States.

The next chapter will use the Global Positioning System as a case study. It was chosen to illustrate how a single platform's vulnerabilities create risk across multiple other platforms and services. There too, system design, programmatic decisions, and system engineering processes combine to complicate the functioning of the acquisitions loop. Applied to the recommendations made in Chapter 3, certain aspects of the loop are shown to function more smoothly, thereby reducing the risk realized by American forces.

---

[41] United States Air Force, "Air Force Basic Doctrine, Organization, and Command," October 14, 2011, 43, http://www.au.af.mil/au/cadre/aspc/l002/pubs/afdd1.pdf.

Chapter 5

Case Study #2: Global Positioning System

Who now dares state with certainty that in future wars this heavy spending will not result in an electronic Maginot line that is weak because of its excessive dependence on a single technology?

Colonel Qiao Liang and Colonel Wang Xiangsui
Chinese People's Liberation Army

I hate GPS. The idea that we are all hooked to a satellite — formerly bought by me to my great resentment — in a semi-synchronous orbit that that doesn't work in certain circumstances, does not work indoors or in valleys in Afghanistan, is ridiculous.

Dr. Ashton Carter

On the afternoon of October 4, 1957, the Soviet Union successfully launched Sputnik into orbit.[1] A few days after the satellite had captured the world's attention, Johns Hopkins physicists George Weiffenbach and William Guier successfully calculated Sputnik's orbital parameters.[2] The Applied Physics Laboratory researchers accomplished this through analysis of the Doppler shift of the signal emitted by the satellite.[3] Frank McClure was their boss, and as chairman of the Applied Physics Laboratory, he had an uncanny ability to see beyond the technical details to practical applications.[4] He reviewed the results of Weiffenback and Guier's findings and challenged them to "invert the solution," which would permit the determination of a receiver's position on the ground

[1] William E Burrows, *This New Ocean: The Story of the First Space Age* (New York: Modern library, 1999), 182.
[2] Richard D. Easton, *GPS Declassified: From Smart Bombs to Smartphones* (Lincoln, Nebraska: Potomac Books, an imprint of the University of Nebraska Press, 2013), 26.
[3] Easton, *GPS Declassified*, 26.
[4] V.L. Pisacane, "A Tribute to Frank T. McClure," *Johns Hopkins APL Technical Digest* 19, no. 1 (1998): 6, http://www.jhuapl.edu/techdigest/td/td1901/pisacane.pdf.

using only the information about the satellite's orbit.[5] Indeed it was possible, and the age of satellite-assisted navigation began.

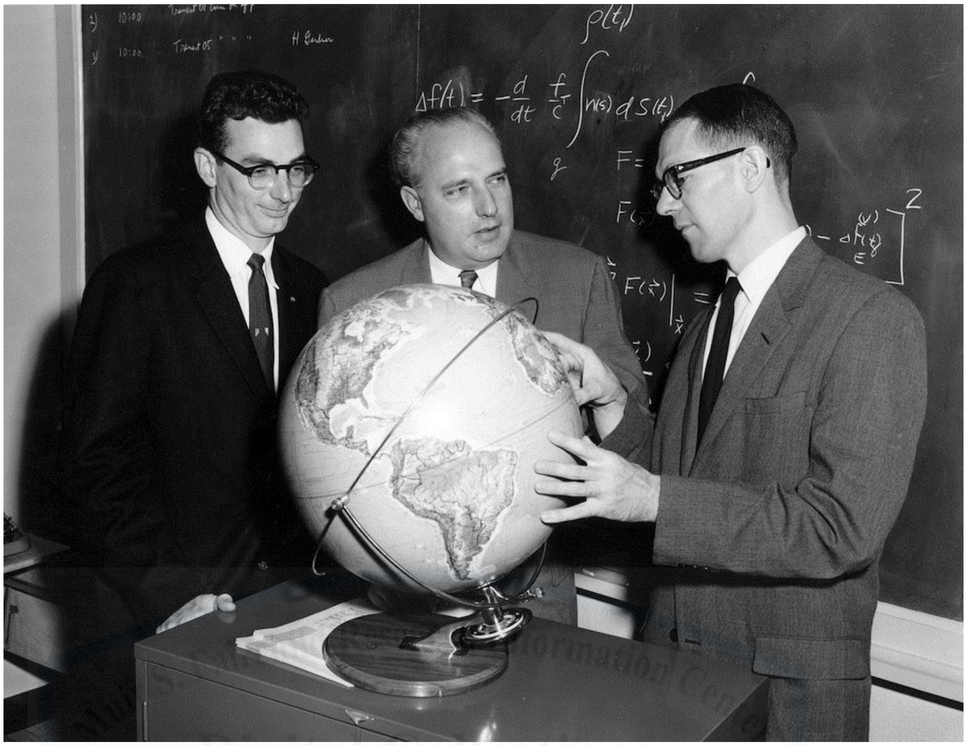

Figure 7: Fathers of GPS
(L to R, William Guier, Frank McClure, and George Weiffenbach)
Photo Courtesy Johns Hopkins University Applied Physics Laboratory

The United States' first satellite navigation system was the Naval Navigation Satellite System, more commonly known as Transit.[6] Fielded in 1964, this system allowed ships and submarines to locate their position anywhere in the world to within approximately 500 feet.[7] This capability was of vital importance to the sea launched ballistic missile mission, which formed the third leg of the nuclear triad.

The Transit system was instrumental in the credibility of America's nuclear deterrent capability but its limitations precluded use on dynamic

---

[5] William Guier and George Weiffenbach, "Genesis of Satellite Navigation," *Johns Hopkins APL Technical Digest* 19, no. 1 (1998): 16, http://www.jhuapl.edu/techdigest/TD/td1901/guier.pdf.
[6] Easton, *GPS Declassified*, 26.
[7] Easton, *GPS Declassified*, 26.

platforms such as aircraft.[8] To overcome these limitations, both the Navy and Air Force explored a number of differing concepts throughout the late 1960s and early 1970s, ultimately settling on the Global Positioning System (GPS).[9] The first operational satellite was launched in 1978, and the 24th satellite—the minimum required to provide uninterrupted, round-the-clock coverage worldwide—did not launch until 1994.[10] Originally intended as a military force multiplier, the importance of GPS has grown and the system is now an indispensible asset to the military, as well as global navigation, communication, and commerce.[11]

As discussed previously, the accuracy of modern navigation and targeting systems allows today's military planners to think very differently than in decades past. Armed with GPS, modern weapons have achieved "near surgical precision," according to Stephen Wrage.[12] "With guided munitions dramatically increasing the likelihood of a single sortie's success, it becomes possible to plan in terms of the number of targets per sortie, thus reversing the historical equation and making possible an economy of force never before seen in air war."[13]

Economy of force was not the only principle of war affected by precision weaponry. In addition to affecting how planners and practitioners alike thought about economy of force, the ability to precisely engage a target also had implications for how to think about achieving the effects of mass. What had historically required massing

---

8 Elliott D. Kaplan, ed., *Understanding GPS: Principles and Applications* (Boston: Artech House, 1996), 2.
9 Kaplan, *Understanding GPS*, 2–3; Easton, *GPS Declassified*, 67.
10 Easton, *GPS Declassified*, 2.
11 Everett C. Dolman, *Astropolitik: Classical Geopolitics in the Space Age*, Cass Series--Strategy and History (London ; Portland, OR: Frank Cass, 2002), 37.
12 Stephen Wrage, "Prospects for Precision Air Power," *Defense and Security Analysis* 19, no. 2 (2003): 102.
13 Keith L. Shimko, *The Iraq Wars and America's Military Revolution* (New York, NY: Cambridge University Press, 2010), 81; George Friedman and Meredith Friedman, *The Future of War: Power, Technology and American World Dominance in the 21st Century* (New York: St. Martin's Griffin, 1998), 278.

physical forces to reach the necessary concentration of combat power at the decisive place and time now required comparatively few.[14]

These trends have affected planning at both the operational and strategic levels. While operational planners plan in terms of the number of targets per sortie, the strategic issue of how large a force to maintain also must be considered.[15] Because a smaller military force can meet the requirements, the size of the military's arsenal has diminished correspondingly. As stated in Chapter 2, the Air Force purchased a total of 744 B-52s compared to only 21 B-2A bombers.[16] Similarly, a total of 867 F-15A/C aircraft were manufactured compared to only 187 operational F-22A Raptors.[17]

These trends are not specific to the Air Force or to the air domain. All of the services in every domain have benefitted significantly from capabilities enabled by GPS. For this reason, the discussion that follows explores how vulnerabilities to GPS, a single space force-enhancement system, dramatically increase risk assumed by a number of different platforms in all of the services. Whereas the preceding F-22 case study analyzed a single platform's vulnerabilities, this explores vulnerabilities to GPS that affect many platforms in many services and domains.

Importance of GPS

Indeed, the benefits of GPS are woven into each service's doctrine and have a pronounced effect on how each has trained and equipped for battle. Decisions at a number of different levels have assumed this

---

[14] Frans P. B. Osinga, *Science, Strategy and War the Strategic Theory of John Boyd* (London; New York: Routledge, 2007), 249; John M. Shalikashvili, *Joint Vision 2010* (Washington, D.C: Chairman of the Joint Chiefs of Staff, July 1996), 17.
[15] Shimko, *The Iraq Wars and America's Military Revolution*, 81; Friedman and Friedman, *The Future of War*, 278.
[16] Marcelle Size Knaack, "Encyclopedia of U.S. Air Force Aircraft and Missile Systems, Volume II," 291; United States Air Force, "B-2 Spirit Fact Sheet."
[17] Steve Davies, *F-15 Eagle and Strike Eagle* (Shrewsbury: Airlife, 2002), 90; Obaid Younossi, ed., *Ending F-22A Production: Costs and Industrial Base Implications of Alternative Options* (Santa Monica, CA: RAND, 2010), iii.

capability would be available. The United States has decided what weapons to procure, how many to procure, and how to train its warriors based on the ability to precisely target the enemy. American tactics, techniques, and procedures also incorporate these same assumptions. Undoubtedly, the military would look and behave much differently without that capability. In short, the size, composition, and operation of the United States military are predicated on reliable access to GPS technology.

The military exists to serve a political master, which has certain assumptions on the capabilities and efficacy of military actions.[18] In recent decades, America's military has demonstrated capabilities far beyond what was previously thought possible.[19] This has conditioned the politicians and the polity it serves to expect this elevated level of performance as a routine matter. However, as discussed above, this level of performance and precision is largely reliant on access to a single technology: GPS. Therefore, in certain circumstances where such access is not assured, the military's ability to perform at the expected levels is tenuous.

The disconnect between expectations and capability is especially troublesome because of inherent limitations of space-based platforms. Specifically, it is prohibitively expensive to modify space hardware while on orbit.[20] Therefore, a viable workaround to a countermeasure deployed against a space-based asset may not exist if it cannot be addressed

---

[18] Carl von Clausewitz, *On War*, trans. and ed. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1989), 87; Rear Adm J. C. USN Wylie, *Military Strategy: A General Theory of Power Control* (Annapolis: Naval Institute Press, 1989), 67; B. H. Liddell Hart, *Strategy*, 2nd Rev. ed. 1967 (Reprint, New York: Penguin, 1991), 335.

[19] Shimko, *The Iraq Wars and America's Military Revolution*, 81.

[20] According to NASA, the cost of STS-103 in December 1999 to repair the Hubble Space Telescope was $205M. Today, due to the retirement of the shuttle fleet, no such repair capability exists. National Aeronautics and Space Administration, "Hubble Facts," October, 1999, http://asd.gsfc.nasa.gov/archive/sm3a/downloads/sm3a_fact_sheets/cost-to-taxpayers.pdf.

exclusively through modification of software controlling the satellite's operation, or through changes to tactics, techniques, or procedures.

GPS System Description and Modernization

Satellites are not designed to have infinite lifespans. For a system like GPS whose satellite design lives range from 7.5-15 years, new satellites periodically launch to replace aging platforms.[21] This replenishment process provides the opportunity for capability enhancement or vulnerability mitigation. The GPS is comprised of three components: the space segment, the control segment, and the user segment.[22] Modernization efforts are currently underway within each segment to ensure future warfighter access to GPS.

The space segment is comprised of the satellites.[23] Currently there are 30 operational satellites in orbit.[24] The oldest of these was launched in 1990, and the newest in March of 2015.[25] Significantly, there are 4 different blocks of satellites, each with a unique hardware configuration and associated vulnerability set.[26]

Older satellites launched until 2004, known as Block IIA/IIR, transmit on two frequencies.[27] The two transmitted signals have inherent jam resistance or are encrypted altogether.[28] Unfortunately, the 10-16 watt signal is very weak by the time it travels almost 20,200 km to reach

---

21 National Coordination Office for Space-Based Positioning, Navigation, and Timing, "Space Segment," March 26, 2015, http://www.gps.gov/systems/gps/space/.
22 Air University (U.S.) et al., *Space Primer* (Maxwell Air Force Base, Ala.: Air University Press, 2009), 218.
23 Air University (U.S.) et al., *Space Primer*, 218.
24 National Coordination Office for Space-Based Positioning, Navigation, and Timing, "Space Segment."
25 National Coordination Office for Space-Based Positioning, Navigation, and Timing, "Space Segment."
26 National Coordination Office for Space-Based Positioning, Navigation, and Timing, "Space Segment."
27 Air University (U.S.) et al., *Space Primer*, 218–225; National Coordination Office for Space-Based Positioning, Navigation, and Timing, "Space Segment."
28 Air University (U.S.) et al., *Space Primer*, 218.

Earth.[29] The signal strength has been said to be "equivalent to a Los Angeles user receiving the light from a 60 watt lightbulb in New York."[30] Because of the weakness of the signal, the system is highly susceptible to jamming despite the jam resistant characteristics of the signals.

The next generation of GPS satellites (Block IIR-M/IIF) added capability to transmit up to two additional signals as well as the capability to increase the transmit power.[31] These measures made jamming the signals more difficult, especially for low-power jammers.[32] Unfortunately, users required upgraded receiver hardware to receive the additional signals. Block III satellites are still being developed and will add yet another signal along with enhanced signal reliability, accuracy, and integrity.[33]

The control segment commands the satellites and ensures their transmitted signals are accurate.[34] It consists of a master and alternate control station in the United States as well as 16 unmanned monitoring stations at various locations throughout the world.[35] Each time the space segment adds capabilities, the control segment must also be upgraded to control the new functionalities. Once fielded, the Next Generation Operational Control System will deliver "full command, control, and mission support capabilities" to Block III satellites with growth capability for future architectures and maintaining backwards compatibility with

---

[29] Easton, *GPS Declassified*, 79; Air University (U.S.) et al., *Space Primer*, 222–223.
[30] National PNT Advisory Board, *Jamming the Global Positioning System - A National Security Threat: Recent Events and Potential Cures*, November 4, 2010, 3, http://www.gps.gov/governance/advisory/recommendations/2010-11-jammingwhitepaper.pdf.
[31] Air University (U.S.) et al., *Space Primer*, 225.
[32] Air University (U.S.) et al., *Space Primer*, 225.
[33] National Coordination Office for Space-Based Positioning, Navigation, and Timing, "Space Segment."
[34] Air University (U.S.) et al., *Space Primer*, 219–220.
[35] National Coordination Office for Space-Based Positioning, Navigation, and Timing, "Control Segment," March 27, 2015, http://www.gps.gov/systems/gps/control/.

previous systems.[36] It is designed to provide significant information assurance improvements over existing control systems, significantly enhancing the system's resilience against cyber threats.[37]

Finally, reception of some the new signals transmitted by Block IIR-M/IIF and newer satellites requires updated receiver hardware. Therefore, upgrades to the user segment are necessary to utilize the new functionalities. A joint service program called the Military GPS User Equipment (MGUE) is developing updated receivers for military hardware to ensure warfighter access to GPS.[38]

Without a doubt, each of the three segments' modernization efforts is necessary and purposeful from a purely capabilities perspective. What the above discussion fails to capture is the investment in time and money required to accomplish the upgrades, which would provide insight into the speed of the acquisitions loop. The chart below provides program funding information (appropriations) for each upgrade for fiscal years 2012-2015, along with initial contract award dates.[39]

---

[36] United States Air Force, "Next Generation Operational Control System (OCX) Factsheet," March 2014, http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=18676.
[37] United States Air Force, "Next Generation Operational Control System (OCX) Factsheet."
[38] United States Air Force, "Military Global Positioning System User Equipment Factsheet," June 2, 2014, http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=18673.
[39] All dollar figures are in then-year dollars.

Segment	Contract Award	FY 2015	FY 2014	FY 2013	FY 2012
Space (GPS III)	2008	$504.968M	$698.874M	$811.902M	$978.418M
Control (OSX)	2007	$299.760M	$383.500M	$371.595M	$390.889M
User (MGUE)	2006	$156.659M	$137.233M	N/A	N/A
Total	-	$961.387M	$1219.607M	$1183.497M	$1369.307M

Figure 8: GPS Modernization Funding
Source: FY 2015 figures taken from National Coordination Office for Space-Based Positioning, Navigation, and Timing, "Fiscal Year 2015 Program Funding," January 13, 2015, http://www.gps.gov/policy/funding/2015/.
FY 2014 figures taken from National Coordination Office for Space-Based Positioning, Navigation, and Timing, "Fiscal Year 2014 Program Funding," August 1, 2014, http://www.gps.gov/policy/funding/2014/.
FY 2013 figures taken from National Coordination Office for Space-Based Positioning, Navigation, and Timing, "Fiscal Year 2013 Program Funding," March 10, 2014, http://www.gps.gov/policy/funding/2013/.
FY 2012 figures taken from National Coordination Office for Space-Based Positioning, Navigation, and Timing, "Fiscal Year 2012 Program Funding," March 10, 2014, http://www.gps.gov/policy/funding/2012/.
Space segment figures incorporate procurement and development costs.
Space segment contract award date found at "GPS Block III Factsheet" (United States Air Force, June 3, 2014), http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=18830.
Control segment contract award date found at Los Angeles Air Force Base Public Affairs, "SMC Announces Contract Award for Next Generation GPS Control Segment," November 21, 2007, http://www.losangeles.af.mil/news/story.asp?id=123076912.
User segment contract award date found at United States Air Force, "Military Global Positioning System User Equipment Factsheet," June 2, 2014, http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=18673.

The figure shows upgrades to GPS have been on contract for 7-9 years, and each year approximately one billion dollars are spent to fund those efforts. To date none have been fielded. As evidenced by the information in Figure 8, the speed of the GPS acquisitions loop is far too slow to react to adversary countermeasures. This is troubling considering reliance on GPS has continued to intensify in the years since initiating the modernization effort. Over that same time frame however, the proliferation of GPS-denial devices increasingly threatens the utility of the upgrades. Experts estimated that "by the end of 2009, more than 100,000" GPS-denial devices had been sold in the United States alone.[40] In November 2010, the National Position, Navigation, and Timing Advisory Board warned "interference threats to GPS are very real and promise to get worse."[41]

Now What?

What, then, can be done about the speed of GPS' acquisitions loop? Adopting all of the recommendations made in Chapter 3 won't change the fact that the system relies on advanced space-based platforms whose hardware cannot be modified or upgraded cost-effectively once on orbit. Similarly, satellite operations are and will continue to be an expensive endeavor. However, implementation of the recommendations can have a dramatic effect on the speed of the acquisitions loop in responding to an adversary countermeasure. The benefits realized by each GPS segment are explored in turn.

Space Segment

As stated previously, the hardware of the space segment cannot be modified once on orbit. However, that is not to say that the segment cannot be upgraded once it has been fielded. It simply means that whatever upgrades occur, they are limited to what's possible with the fielded hardware. Establishing alternative contractual requirements and adopting some of the Defense Science Board recommendations discussed in Chapter 3 will accelerate the speed of the acquisitions loop in accomplishing those types of upgrades to the space segment.

---

[40] Callan James, "Precision Approaches," *Avionics Magazine*, November 1, 2011, http://www.aviationtoday.com/av/issue/feature/Precision-Approaches_74764.html#.VRs-oFwTvIY.

[41] National PNT Advisory Board, *Jamming the Global Positioning System - A National Security Threat: Recent Events and Potential Cures*, 10.

The space segment would benefit most from the establishment of a performance parameter that specifies the maximum timeframe allowed for modifying the system would address a substantial system vulnerability. Doing so would result in hardware designed to be more versatile. This would allow for performance parameters of the system to be changed while the satellite is in orbit. Unfortunately, this is not an option for the systems already fielded but can dramatically enhance the resilience of the GPS constellation moving forward.

An example of how this would be implemented involves the antennas and supporting hardware. Much of the hardware associated with the antennas on the GPS satellites is optimized to operate on the pre-established downlink frequencies. Knowledge of these frequencies greatly simplifies the adversary's task when attempting to jam the signals. Having hardware that can acceptably operate on many different frequencies would permit a frequency-agile signal over a wider bandwidth, further complicating the adversary's task.[42] Admittedly, cost increases and performance tradeoffs are associated with this particular example that might make it less than desirable, but it illustrates the point nonetheless.

Recommendations made by the Defense Science Board can also assist in speeding up the acquisitions loop for the GPS space segment. Improved strategic intelligence and red teaming by an engineering team kept in warm status would complement the capabilities provided by versatile satellite hardware. First, strategic intelligence would characterize what the threat is working towards, decreasing the threat of capability surprise. Red teaming would allow the information from the strategic intelligence to be incorporated into potential solutions, which could then be verified in a test environment. Together, improved intelligence and red teaming could arrive at solutions that best address

---

[42] David Adamy, *EW 101: A First Course in Electronic Warfare*, Artech House Radar Library (Boston: Artech House, 2001), 125–129.

adversary countermeasures. Then, when such countermeasures are fielded, the fix will be readily available ensuring warfighter access to GPS is maintained.

Control Segment

Unlike the space segment, the control segment has a significant advantage over the fielded satellites in that both the hardware and software can be upgraded or modified. Whatever changes do take place, however, must maintain compatibility with the satellites on orbit. The speed of the acquisitions loop for the control segment would benefit from an engineering red team kept in warm status, alternative contractual requirements, as well as "good enough" solutions proposed in Chapter 3.

The speed of the acquisitions loop can be accelerated with an engineering team that remains in warm status. This team would ensure the proper expertise is available to respond to capability surprises. Additionally, the team would participate in red teaming, leveraging enhanced strategic intelligence to enhance system resiliency.

Alternative contractual requirements would also speed up the control segment's acquisitions loop. Understanding the results of contractor independent research and development efforts could enable senior leaders to field available solutions quickly that work in lieu of developing entirely new capabilities from scratch. The control segment can also benefit from establishing a performance parameter tied to the speed of modification. This would ensure that future systems can more quickly respond to adversary countermeasures to ensure the control segment can continue providing support to the space segment.

Just like any technological system, the control segment requires a basic level of functionality. There are certain things that it must be able to do. Other tasks may not be as critical or time sensitive. Therefore, when addressing adversary countermeasures, accepting "good enough" for a short time can ensure some level of GPS access to the warfighter. Certainly over time, most of the capability will require restoration.

User Segment

The user segment is different from the space and control segments. First and foremost, it is everywhere and is not centrally controlled or funded. The aforementioned modernization program is only developing receiver hardware to ensure military access to GPS and will have little to no direct effect on civilian GPS access.[43] Nonetheless, the acquisitions loop of this segment can also benefit from recommendations made in Chapter 3.

Engineers supporting the joint service program developing the military receiver hardware should be kept in warm status in order to realize the same benefits discussed for the space and control segments. The vulnerabilities to the user segment can also be decreased with the alternative contractual requirements proposed earlier. Additionally, the user segment can benefit from adopting "good enough" solutions, whose selection would accelerate the acquisitions loop and likely decrease the overall cost of fielding a solution.

Where the user segment would probably benefit most is from the recommendations made by the Defense Science Board regarding the fulfillment of urgent operational needs. The board recommended a dual acquisitions path and separate funding streams for rapid acquisition programs. In the event an upgrade or modification to the user segment is necessary, these recommendations are perfectly suited to fund the program. This is largely because the Rapid Acquisition and Fielding Agency would relieve the weapon system's program office from the burden of making cost, schedule, and performance tradeoffs from within

[43] United States Air Force, "Military Global Positioning System User Equipment Factsheet."

the program which would certainly delay fielding of the upgrade or modification.

Conclusion

The United States has decided what weapons to procure, how many to procure, and how to train its warriors based on the ability to precisely target the enemy. The ability to achieve such precision is largely reliant on access to a single technology: GPS. The size, composition, and operation of the United States military are predicated on reliable access to GPS technology. In many respects, GPS has become the single technology forming an "electronic Maginot line" referred to by Chinese Colonels Qiao Liang and Wang Xiangsui.[44] For those same reasons, it is why Secretary of Defense Dr. Ashton Carter has said that he "hates" it.[45]

Strangely, vulnerabilities to GPS create risk for other platforms. In the extreme, they jeopardize America's abilities to conduct military operations in the manner for which it has prepared and equipped itself. Therefore, reliable access to GPS is a vital interest and is inextricably linked to the speed of the GPS acquisitions loop.

This chapter explored how the recommendations made in Chapter 3 can improve the speed of the GPS acquisitions loop. While previous decisions on system design create many of today's vulnerabilities, future designs can benefit greatly from designs that place a premium on system versatility across all three GPS segments. Ensuring engineering expertise remains available and engaged through red teaming will decrease the time required to respond to an adversary countermeasure. Finally, settling on intermediate acceptable solutions for compromised control or user segments can ensure access to GPS while more robust solutions are

---

[44] Liang, Qiao and Xiangsui, Wang, *Unrestricted Warfare* (Beijing, China: PLA Literature and Arts Publishing House, February 1999), 87.

[45] Michael Copeland, "How Government Drives Innovation: An Interview with Ashton Carter," June 24, 2014, http://a16z.com/2014/06/24/how-government-drives-innovation-a-conversation-with-former-deputy-secretary-of-defense-ashton-carter/.

developed. Capitalizing on flexible and adaptable funding and oversight mechanisms proposed by the Defense Science Board would also accelerate the speed of the acquisitions loop.

Chapter 6

Conclusion

In recent decades, the United States military has become substantially more lethal and effective while it has shrunk in size. The changes have been so dramatic that American military planners today think about the principles of mass and economy of force using an entirely different framework than their predecessors did. Advancements in technology were a driving force for these changes, fulfilling a long-standing social mandate to minimize both the cost and collateral damage of war. Technology in warfare is here to stay.

Advanced technology has proven itself as a force multiplier and has affected the military in profound ways. It's ability to engage the adversary with unmatched precision has dramatically changed the military's force structure as well as its tactics, techniques, and procedures. The military expects the technology fueling its weapons to function properly, and has altered how the United States trains and fights. This study sought to explore the relationship between technology and strategic risk by answering the question: Does the military's growing reliance on technology translate into a strategic liability?

For a number of reasons, technology as it is currently implemented can be a strategic liability for the military. Some of the reasons for this are technological and have their roots in the architecture of the weapon systems themselves. Other reasons stem from structural factors rooted in how the acquisition system works, specifically as it pertains to how upgrades and modifications are developed and fielded. This research effort identified that the growth of technology-dependent weapons carries four implications that introduce vulnerabilities or increase risk. Each implication is noteworthy individually. However, it is important to highlight that they have a cumulative effect and together are a veritable house of cards with a fragile foundation.

First, because of the system architecture, potential adversaries are able to attack a weapon system via any number of access points, realizing effects that previously would have required the efforts of a great power. Second, the incredible strength of America's military virtually invites an increasingly asymmetric threat and enhances the effects an asymmetric attack can realize. Third, because technologically-advanced weapons are generally more capable and more expensive than their primitive counterparts, there are fewer of them. The comparatively small number of weapons is itself a vulnerability. Finally, when an adversary deploys a countermeasure affecting a weapon system capability, often times a modification is required to the system's hardware, software, or both. Such modifications rely on the speed of the acquisition loop.

Taken together, these implications present significant, yet manageable, challenges for the strategist. In the extreme, the crippling of a low density, high demand platform could result in strategic paralysis. The likelihood of this happening is affected by decisions made in the platform's design as well as by the process used to upgrade or modify the system. Redesigning all of America's military hardware is both impractical and would be prohibitively expensive. Furthermore, it wouldn't eliminate all of the vulnerabilities associated with technologically-advanced weapon systems. Therefore, the path to resiliency seeks to optimize the process used to upgrade or modify existing weapon systems. For weapon systems not yet fielded, it is equally critical that their design accommodate realities of the modern battlefield. This study focused on ways to accomplish these two tasks.

Not surprisingly, this is not a new problem and fortunately significant scholarship existed for this study to build upon. The Defense Science Board convened two separate, but related, studies in 2009. One examined Capability Surprise and the other examined the Fulfillment of

Urgent Operational Needs. Adoption of the recommendations made by both studies would greatly benefit the problem under consideration by this study.

The Defense Science Board Capability Surprise study made the following four recommendations:

1. Establish a Capability Assessment, Warning, and Response Office (CAWRO) to provide DoD senior leadership with timely assessment and warning of potentially high-risk adversary capabilities, with options for addressing them.

2. Red team to address strategic level issues, and as part of major acquisitions, exercises, and developmental education.

3. Establish a standing Rapid Capability Fielding Office (RCFO) to improve DoD capabilities for addressing priority surprise capability gaps and supporting urgent war fighter needs.

4. Improve strategic intelligence to provide insight into adversary capabilities, intent, vulnerabilities, and denial and deception efforts.[1]

The board examining the Fielding of Urgent Operational Needs made the following recommendations:

1. The Secretary of Defense should formalize a dual acquisition path.

2. Executive and Legislative branches must establish a fund for rapid acquisition and fielding.

3. The Secretary of Defense should establish a new agency with a proposed name of Rapid Acquisition and Fielding Agency (RAFA). The agency will be "focused on speed, utilizing existing technologies, and acquisition flexibilities to achieve a 75 percent solution initially 'good enough' to address the urgent needs of the warfighter."

[1] Defense Science Board, *Capability Surprise*, September 2009, xiv-xv, http://www.acq.osd.mil/dsb/reports/ADA506396.pdf.

4. Initial billets and funding for RAFA will be based on absorbing and integrating existing programs and organizations.

5. DoD should establish a streamlined, integrated approach for rapid acquisition.[2]

Indeed, adopting the recommendations from either or both studies would accelerate the speed of America's overall acquisition loop. Both panels identified and recommended creating pathways to circumvent the crippling bureaucracy of the traditional acquisition processes. However, they fail to acknowledge explicitly the very real possibility that a weapon system may be crippled until a viable counter-countermeasure is fielded.

For that reason, this study recommends three additional measures beyond those proposed by the two Defense Science Board studies:

1. Maintain a viable development capability in "warm" status throughout the life of a technologically advanced weapon system.

2. Consider alternative contractual requirements to ensure the acquisition loop can cycle as fast as possible.

3. Reintroduce the concept of 'good enough' to improve the speed of the acquisitions loop, as the pursuit of nearly perfect solutions significantly slows the speed of the acquisitions loop.

The case study of the F-22 highlights how its architecture and reliance on technology is emblematic of trends in modern weaponry. While both of these characteristics result in levels of precision and lethality never before seen, they also introduce a whole host of vulnerabilities to the weapon system. Were an adversary to attack one of the vulnerabilities, the effects would likely be limited to the F-22. To

---

[2] Defense Science Board, *Fulfillment of Urgent Operational Needs*, July 2009, x-xii, http://www.acq.osd.mil/dsb/reports/ADA503382.pdf.

restore the lost capabilities, the military would naturally turn to the acquisitions system to engineer an upgrade or modification.

The F-22 is vitally important to the Air Force's ability to provide its doctrinal core function of air superiority. Were an adversary to attack the ability of the F-22 to fully function on the battlefield, the Air Force's ability to provide its doctrinal core function would rely on the speed of the acquisitions loop. The recommendations made by the Defense Science Board make great contributions to accelerating the speed of the acquisitions loop. The additional recommendations made in this study aim to further accelerate its operation by ensuring the weapons system is designed for such an eventuality and the acquisitions system is primed to respond to an adversary attack.

The Global Positioning System (GPS) case study highlights how an adversary attack on a single platform can realize effects across many other platforms, in all the services, and in all domains. The United States military has become so reliant on GPS that its force structure, doctrine, and operations all largely assume access to GPS. If that is denied by an adversary attack, our military readiness could be dramatically impacted virtually overnight. Again, the speed of the acquisitions loop becomes critical in America's ability to respond to such an attack. The recommendations made by the Defense Science Board and this study seek to enhance our ability to respond in such a scenario and increase the resiliency of future GPS hardware.

The overwhelming might of the United States military is increasingly dependent upon properly functioning technology. This dependency results in greater vulnerabilities and assumes increased risk in a number of critical areas. Our adversaries are going to attack our technological advantage. The effects of their attacks can be decreased if the United States ensures its acquisitions loop can respond to these attacks so as to prevent strategic paralysis and ensure the full force of our military capability continues to remain fully within our control.

Bibliography

Academic Papers

David S. Fadok. "John Boyd and John Warden: Air Power's Quest for Strategic Paralysis." School of Advanced Airpower Studies, 1995.

LaFleur, Jeffrey. "Tear Down the Wall Chart: Rapid Acquisitions for the Rest of the Department of Defense." Air Force Research Institute, 2012.

Liang, Qiao, and Xiangsui, Wang. *Unrestricted Warfare*. Beijing, China: PLA Literature and Arts Publishing House, February 1999. http://www.terrorism.com/documents/unrestricted.pdf.

Thornhill, Paula G. *Over Not Through: The Search for a Strong, Unified Culture for America's Airmen*. RAND Corporation Occasional Paper Series OP-386-AF. Santa Monica, CA: Rand, 2012.

Books

Adamy, David. *EW 101: A First Course in Electronic Warfare*. Artech House Radar Library. Boston: Artech House, 2001.

Air University (U.S.), Air Command and Staff College, Air University (U.S.), and Press. *Space Primer*. Maxwell Air Force Base, Ala.: Air University Press, 2009.

Aronstein, David C., Michael J. Hirschberg, and Albert C. Piccirillo. *Advanced Tactical Fighter to F-22 Raptor Origins of The 21st Century Air Dominance Fighter*. Reston, Va.: American Institute of Aeronautics and Astronautics, 1998.

Augustine, Norman R. *Augustine's Laws*. 6th ed. Reston, VA: American Institute of Aeronautics and Astronautics, 1997.

Biddle, Tami Davis. *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas About Strategic Bombing, 1914-1945*. Princeton, N.J.: Princeton University Press, 2002.

Burrows, William E. *This New Ocean: The Story of the First Space Age*. New York: Modern library, 1999.

Clarke, Richard A. *Cyber War: The Next Threat to National Security and What to Do About It*. 1st Ecco pbk. ed. New York: Ecco, 2012.

Clausewitz, Carl von. *On War*. Trans. and ed. Michael Howard and Peter Paret. Princeton, N.J.: Princeton University Press, 1989.

Davies, Steve. *F-15 Eagle and Strike Eagle*. Shrewsbury: Airlife, 2002.

Dolman, Everett C. *Astropolitik: Classical Geopolitics in the Space Age*. Cass Series--Strategy and History. London ; Portland, OR: Frank Cass, 2002.

Easton, Richard D. *GPS Declassified: From Smart Bombs to Smartphones*. Lincoln, Nebraska: Potomac Books, an imprint of the University of Nebraska Press, 2013.

Flichy, Patrice. *Understanding Technological Innovation: A Socio-Technical Approach*. Cheltenham, UK; Northampton, MA: Edward Elgar, 2007.

Friedman, George, and Meredith Friedman. *The Future of War: Power, Technology and American World Dominance in the 21st Century*. New York: St. Martin's Griffin, 1998.

Gentry, John A. *How Wars Are Won and Lost: Vulnerability and Military Power*. Santa Barbara, CA: Praeger Security International, 2012.

Gray, Colin S. *Modern Strategy*. New York: Oxford University Press, 1999.

———. *Perspectives on Strategy*. 1st ed. Oxford, U.K: Oxford University Press, 2013.

Guilmartin, John F. "Technology and Asymmetrics in Modern Warfare." In *Challenging the United States Symmetrically and Asymmetrically: Can America Be Defeated?*, edited by Lloyd J. Matthews. Carlisle Barracks, Pennsylvania: U.S. Army War College, 1998. http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB230.pdf.

Hammes, Thomas X. *The Sling and The Stone: On War in The 21st Century*. Minneapolis, MN: Zenith, 2006.

Hammond, Grant Tedrick. *The Mind of War: John Boyd and American Security*. Washington: Smithsonian Institution Press, 2001.

Hart, B. H. Liddell. *Strategy*. 2nd Rev. ed. 1967. Reprint, New York: Penguin, 1991.

Henriksen, Dag. *NATO's Gamble: Combining Diplomacy and Airpower in the Kosovo Crisis, 1998-1999*. Annapolis, MD: Naval Institute Press, 2007.

J. Ronald Fox. *Defense Acquisition Reform, 1960-2009; An Elusive Goal*. Washington, D.C: Center of Military History, 2011.

Kaplan, Elliott D., ed. *Understanding GPS: Principles and Applications*. Boston: Artech House, 1996.

Kilcullen, David. *Out of the Mountains: The Coming Age of the Urban Guerrilla*. 1 edition. Oxford ; New York, NY: Oxford University Press, 2013.

McShea, Robert E. *Test and Evaluation of Aircraft Avionics and Weapon Systems*. AIAA Education Series. Raleigh, NC : Reston, Va: SciTech Publishing ; American Institute of Aeronautics and Astronautics, 2010.

Merriam-Webster, Inc. *Merriam-Webster's Collegiate Dictionary*. 11th ed. Springfield, Mass: Merriam-Webster, Inc, 2003.

Osinga, Frans P. B. *Science, Strategy and War the Strategic Theory of John Boyd*. London; New York: Routledge, 2007.

Rosen, Stephen Peter. *Winning the Next War: Innovation and the Modern Military*. Ithaca: Cornell University Press, 1991.

Sherry, Michael S. *The Rise of American Air Power: The Creation of Armageddon*. New Haven: Yale University Press, 1987.

Shimko, Keith L. *The Iraq Wars and America's Military Revolution*. New York, NY: Cambridge University Press, 2010.

Simpson, Emile. *War From the Ground Up: Twenty-First Century Combat as Politics*. Oxford ; New York, NY: Oxford University Press, 2012.

Singer, P. W. *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century*. New York: Penguin Books, 2010.

Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, NY: Oxford University Press, 2014.

Stephen Wrage. "Prospects for Precision Air Power." *Defense and Security Analysis* 19, no. 2 (2003): 101–9.

Tzu, Sun. *The Illustrated Art of War: The Definitive English Translation by Samuel B. Griffith*. New York: Oxford University Press, 2005.

United States Air Force Academy. *Contrails*. Vol. 1996–97. USAFA, CO, 1996.

Wakelam, Randall T. *The Science of Bombing: Operational Research in RAF Bomber Command*. Toronto ; Buffalo: University of Toronto Press, 2009.

Walzer, Michael. *Just And Unjust Wars: A Moral Argument With Historical Illustrations*. 4th ed. New York: Basic Books, 2006.

Ward, Dan. *F.I.R.E.: How Fast, Inexpensive, Restrained, and Elegant Methods Ignite Innovation*. First edition. New York: Harper Business, 2014.

Wylie, Rear Adm J. C. USN. *Military Strategy: A General Theory of Power Control*. Annapolis: Naval Institute Press, 1989.

Younossi, Obaid, ed. *Ending F-22A Production: Costs and Industrial Base Implications of Alternative Options*. Santa Monica, CA: RAND, 2010.

Articles

Adee, S. “The Hunt For The Kill Switch.” *Spectrum, IEEE* 45, no. 5 (2008): 34–39. doi:10.1109/MSPEC.2008.4505310.

Arthur K. Cebrowski, and John H. Garstka. “Network-Centric Warfare - Its Origin and Future.” *Proceedings Magazine*, January 1998. http://www.usni.org/magazines/proceedings/1998-01/network-centric-warfare-its-origin-and-future.

Callan James. “Precision Approaches.” *Avionics Magazine*, November 1, 2011. http://www.aviationtoday.com/av/issue/feature/Precision-Approaches_74764.html#.VRs-oFwTvIY.

Charles J. Dunlap Jr. “21st-Century Land Warfare: Four Dangerous Myths.” *Parameters*, Autumn 1997, 27–37.

Fulghum, David A., Robert Wall, and Amy Butler. “Cyber-Combat’s First Shot.” *Aviation Week & Space Technology* 167, no. 21 (November 26, 2007): 28–31.

Gates, Robert M. “A Balanced Strategy.” *Foreign Affairs*, January 1, 2009. http://www.foreignaffairs.com/print/63717.

Kelly, Michael. “The American Way of War.” *The Atlantic*, June 2002. http://www.theatlantic.com/magazine/archive/2002/06/the-american-way-of-war/302513/.

Michael Copeland. “How Government Drives Innovation: An Interview with Ashton Carter,” June 24, 2014. http://a16z.com/2014/06/24/how-government-drives-innovation-a-conversation-with-former-deputy-secretary-of-defense-ashton-carter/.

Paul Kennedy. “The Greatest Superpower Ever.” *New Perspectives Quarterly* 19, no. 2 (Spring 2002). http://www.digitalnpq.org/archive/2002_spring/kennedy.html.

V.L. Pisacane. “A Tribute to Frank T. McClure.” *Johns Hopkins APL Technical Digest* 19, no. 1 (1998). http://www.jhuapl.edu/techdigest/td/td1901/pisacane.pdf.

William Guier, and George Weiffenbach. “Genesis of Satellite Navigation.” *Johns Hopkins APL Technical Digest* 19, no. 1 (1998). http://www.jhuapl.edu/techdigest/TD/td1901/guier.pdf.

Briefings/Point Papers/Memos/Online Content

Defense Acquisitions University. “Defense Manufacturing Management Guide for Program Managers, Chapter 5.6 Reliability, Availability, and Maintainability.” Defense Acquisitions University, July 5, 2012. https://acc.dau.mil/communitybrowser.aspx?id=520790.

"FAQs." *F-35 Lightning II*. Accessed January 30, 2015. https://www.f35.com/resources/faqs.

"GPS Block III Factsheet." United States Air Force, June 3, 2014. http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=18830

Guy Eastman, and Fenella McGerty. "US No Longer Spends More on Defense than Next 10 Biggest Countries Combined." *IHS Jane's 360*, June 25, 2014. http://www.janes.com/article/40083/analysis-us-no-longer-spends-more-on-defense-than-next-10-biggest-countries-combined.

Lockheed Martin. "Lockheed Martin Delivers Final, Historic F-22 Raptor to U.S. Air Force." *Lockheed Martin Press Release*, May 2, 2012. http://www.lockheedmartin.com/us/news/press-releases/2012/may/120502ae_final-f-22-delivered.html.

Los Angeles Air Force Base Public Affairs. "SMC Announces Contract Award for Next Generation GPS Control Segment," November 21, 2007. http://www.losangeles.af.mil/news/story.asp?id=123076912.

National Coordination Office for Space-Based Positioning, Navigation, and Timing. "Control Segment," March 27, 2015. http://www.gps.gov/systems/gps/control/.

———. "Fiscal Year 2012 Program Funding," March 10, 2014. http://www.gps.gov/policy/funding/2012/.

———."Fiscal Year 2013 Program Funding," March 10, 2014. http://www.gps.gov/policy/funding/2013/.

———. "Fiscal Year 2014 Program Funding," August 1, 2014. http://www.gps.gov/policy/funding/2014/.

———. "Fiscal Year 2015 Program Funding," January 13, 2015. http://www.gps.gov/policy/funding/2015/.

———. "Space Segment," March 26, 2015. http://www.gps.gov/systems/gps/space/.

National PNT Advisory Board. *Jamming the Global Positioning System - A National Security Threat: Recent Events and Potential Cures*, November 4, 2010. http://www.gps.gov/governance/advisory/recommendations/2010-11-jammingwhitepaper.pdf.

Phil Damon. "F-22 Joint Procedure 035: Operational and Flight Clearance Approval and Documentation," July 3, 2014.

———. "B-2 Spirit Fact Sheet," April 1, 2005. http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104482/b-2-spirit.aspx.

———. "Military Global Positioning System User Equipment Factsheet," June 2, 2014.

http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=18673.

———. "Next Generation Operational Control System (OCX) Factsheet," March 2014. http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=18676.

Government Documents

Jeremiah Gertler. *Air Force F-22 Fighter Program: Background and Issues for Congress*. Washington, D.C.: Congressional Research Service, December 22, 2009. http://www.au.af.mil/au/awc/awcgate/crs/rl31673.pdf.

John M. Shalikashvili. *Joint Vision 2010*. Washington, D.C: Chairman of the Joint Chiefs of Staff, July 1996.

"Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms," November 14, 2014. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

Marcelle Size Knaack. "Encyclopedia of U.S. Air Force Aircraft and Missile Systems, Volume II." United States Air Force Office of Air Force History, 1988. http://www.afhso.af.mil/shared/media/document/AFD-100526-026.pdf.

United States Air Force. "Air Force Basic Doctrine, Organization, and Command," October 14, 2011. http://www.au.af.mil/au/cadre/aspc/l002/pubs/afdd1.pdf.

Personal Communications – Interviews/E-Mails

Charles Staley. Personal communication, January 9, 2015.

Dr. Camron Gorguinpour. Director of Transformational Innovation. Telephone, February 26, 2015.

Chris Gentile. United States Air Force Rapid Capabilities Office Program Manager. Telephone, February 26, 2015.

Reports

Defense Science Board. *Capability Surprise*, September 2009. http://www.acq.osd.mil/dsb/reports/ADA506396.pdf.

———. *Defense Science Board Task Force On High Performance Microchip Supply*, February 2005. http://www.acq.osd.mil/dsb/reports/ADA435563.pdf.

———. *Fulfillment of Urgent Operational Needs*, July 2009. http://www.acq.osd.mil/dsb/reports/ADA503382.pdf.